Universidade de Aveiro Departamento de Matemática

2007

ANTÓNIO FERREIRA PEREIRA

ALGORITMOS E COMPLEXIDADE NO MODELO DE COMPUTAÇÃO QUÂNTICA

Universidade de Aveiro Departamento de Matemática
2007

ANTÓNIO FERREIRA PEREIRA

ALGORITMOS E COMPLEXIDADE NO MODELO DE COMPUTAÇÃO QUÂNTICA

tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Matemática, realizada sob a orientação científica da Doutora Maria Rosália Dinis Rodrigues, Professora Associada do Departamento de Matemática da Universidade de Aveiro

À magia
nos teus olhos

o júri

presidente

Doutor José Rodrigues Ferreira da Rocha
Professor Catedrático da Universidade de Aveiro

vogais

Doutor Jesús García López de Lacalle
Professor Catedrático da Escuela Universitária de Informática da Universidade Politécnica de Madrid

Doutor José Fernando Ferreira Mendes
Professor Catedrático da Universidade de Aveiro

Doutor Domingos Moreira Cardoso
Professor Catedrático da Universidade de Aveiro

Doutora Maria Rosália Dinis Rodrigues
Professora Associada da Universidade de Aveiro (Orientadora)

Doutor Paulo Alexandre Carreira Mateus
Professor Auxiliar com Agregação do Instituto Superior Técnico da Universidade Técnica de Lisboa

agradecimentos

À minha orientadora Doutora Rosália Rodrigues que sempre me incutiu o espírito da investigação. A ela o meu sincero agradecimento. Jamais esquecerei a sua constante amizade, disponibilidade, apoio e incentivo.

Ao Departamento de Matemática da Universidade de Aveiro, pelas excelentes condições de trabalho proporcionadas.

À Unidade de I&D Centro de Estudos em Optimização e Controlo, pelo apoio financeiro prestado.

A todos os meus colegas do departamento, incluindo funcionários, pelo ambiente de trabalho proporcionado.

Aos meus pais, irmãs e irmãos, pelo carinho constante.

Aos meus amigos, por me suportarem nos momentos menos bons.

palavras-chave

computação quântica, redundância, aritmética, algoritmos, circuitos, complexidade, qudits

resumo

Nesta tese estudam-se as implicações da introdução no modelo de Computação Quântica do conceito de Sistema de Representação Redundante, em particular no que concerne à eficiência de Algoritmos para Aritmética.

Têm vindo a ser apresentadas diversas considerações favoráveis sobre a exequibilidade de modelos de Computação Quântica em que a unidade de informação, o qudit, admite mais do que os dois níveis distintos proporcionados pelo qubit. O problema da equivalência, ou não, em termos de Complexidade Computacional entre modelos baseados em qubits e aqueles baseados em qudits encontra-se apenas parcialmente resolvido.

A análise da Complexidade Computacional de modelos em que se consideram misturas de diferentes unidades de informação, denominados Sistemas Quânticos Híbridos, é uma área praticamente inexplorada. Assim, propõe-se um modelo formal para Computação Quântica nestes sistemas híbridos, generalizando, por inclusão, os modelos baseados em qubits e qudits.

Com base no modelo proposto, desenvolvem-se duas classes de circuitos quânticos, com profundidade constante, para a adição das representações de dois números num qualquer sistema redundante. Estabelecem-se ainda condições para a aplicação de um algoritmo de adição, em tempo constante, de um número polinomial de representações redundantes de números. Como consequência, justifica-se a existência de classes de circuitos quânticos, com profundidade constante, para aproximar a soma de um número polinomial de representações redundantes.

Por fim, descrevem-se as principais características de um Simulador Simbólico para Algoritmos em Computação Quântica, seguindo-se uma análise de resultados obtidos em simulações do algoritmo de Grover.

keywords quantum computation, redundancy, arithmetic, algorithms, circuits, complexity, qudits

abstract

In this thesis we study the effect of merging the concept of Redundant Number Systems with Quantum Computation, manly with respect to Quantum Arithmetic Algorithms.

Several favorable opinions have been advanced on the feasibility of Quantum Computation models where the unit of information, the qudit, has more than the two levels provided by the qubit. However, the equivalence between this model and the qubit based one is only partially established.

The Computational Complexity analysis of Hybrid Quantum Computation models where mixtures of several, distinct, units of information coexist has just started. We propose a new and general formal model for Quantum Computation with Hybrid Quantum Systems, generalizing, by inclusion, all the above mentioned models.

Based on this model, we report two classes of constant depth quantum circuits for the addition of two numbers in redundant number systems.
Also, we derive conditions for the feasibility of addition, in constant time, of a polynomial number of numbers (represented in any redundant number system) and justify the existence of constant depth quantum circuits for approximating the sum of a polynomial number of numbers.

Finally, we report the development of a Symbolic Quantum Computer Simulator and discuss the time-results of the simulation of Grover's algorithm.

Índice

Lista de Figuras

Lista de Símbolos

$\emptyset$ Conjunto vazio.

Γ Linguagem ou alfabeto.

$\mathbb{N}$ Conjunto dos inteiros positivos.

$\mathbb{Z}$ Conjunto dos inteiros.

$\mathbb{C}$ Corpo dos números complexos.

$\mathbb{Z}_d$ Para $d \geq 2$, denota o conjunto $\{k \in \mathbb{Z}, 0 \leq k < d\}$.

$\mathbf{U}$ Operador unitário.

$[m \,..\, n]$ Para $m, n \in \mathbb{Z}$, denota o conjunto $\{k \in \mathbb{Z}, m \leq k \leq n\}$. Para $m > n$, $[m \,..\, n] = \emptyset$.

$\langle \_ | \_ \rangle$ Produto interno. Acção de um *bra* sobre um *ket*.

$\langle \_ |$ Bra: funcional linear num espaço de Hilbert.

$| \_ \rangle$ Ket: elemento de um espaço de Hilbert, geralmente com norma 1.

$\mathcal{H}$ Espaço de Hilbert.

$\mathcal{V}$ Espaço vectorial.

$\mathcal{U}(\mathcal{H})$ Conjunto dos operadores lineares no espaço de Hilbert $\mathcal{H}$.

$\otimes$ Produto tensorial.

$\cong$ Isomorfismo.

$\equiv$ Equivalência entre notações ou designações.

$\dagger$ Para um operador $\mathbf{A}$, $\mathbf{A}^\dagger$ denota o operador adjunto de $\mathbf{A}$. Se $\mathcal{H}$ é um espaço de Hilbert , $\mathcal{H}^\dagger$ denota o espaço dual de $\mathcal{H}$.

$\setminus$ Complementar de um conjunto.

$\bigotimes_{i=1}^{n}$ Produto tensorial iterado. A ordem dos factores é $\bigotimes_{i=1}^{n} a_j = a_1 \otimes a_2 \otimes \cdots \otimes a_n$.

Prelúdio

Na tese de Church, formulada por volta de 1930, diz-se essencialmente que qualquer função computável é computável por uma máquina de Turing. Esta conjectura surge na sequência de demonstrações de equivalência entre vários modelos de computação aparentemente distintos. A ligação entre o modelo matemático abstracto da máquina de Turing com a Física foi despoletada em 1982, por Feynman, ao salientar a aparente intratabilidade da simulação de processos da Mecânica Quântica e posteriormente formalizada por David Deutsch naquela que ficou conhecida por Tese Forte de Church-Turing.

Em última instância qualquer computação é realizada por um sistema físico, seja ele um sistema clássico ou quântico. Por essa altura, assiste-se ao traçar inicial de um novo modelo de computação baseado nas leis da Física Quântica, a Computação Quântica.

Desde então, esta área tem sido alvo de investigação fortemente activa, nomeadamente após os resultados surpreendentes obtidos por Peter Shor sobre a possibilidade de resolver em tempo polinomial, num (hipotético) computador quântico, certos problemas para os quais não se conhecem algoritmos clássicos eficientes.

A Computação Quântica evoluiu entretanto para uma vasta área de interacção com outras áreas do conhecimento, entre as quais se destacam a Física Quântica e a Computação Clássica em subáreas como a Teoria da Complexidade e o desenvolvimento de Algoritmos, entre outras.

Se por exagero se diz que a Computação Clássica é a ciência do bit então por analogia a Computação Quântica é actualmente a ciência do qubit.

Várias considerações foram entretanto apresentadas sobre a exequibilidade de fundamentar a Computação Quântica para sistemas quânticos em que a unidade de informação, o qudit,

admite mais do que os dois níveis distintos do qubit.

Não é de todo evidente a equivalência entre modelos de computação baseados em qubits e modelos baseados em qudits, muito menos em que termos se poderá definir uma tal equivalência. As dificuldades agravam-se quando se consideram sistemas de computação em misturas de diferentes unidades de informação, denominados sistemas quânticos híbridos.

A motivação subjacente ao trabalho de investigação realizado é a questão de clarificar as consequências gerais da introdução do conceito clássico de Sistema de Representação Redundante na área da Computação Quântica, em particular no que concerne à eficiência de Algoritmos para Aritmética.

Desde o início que se tornou evidente a necessidade fundamentar os resultados obtidos sob um modelo para Computação Quântica em sistemas híbridos, até então inexistente. Assim, no capítulo 2 alicerça-se a construção de um possível modelo que generaliza, por inclusão, os modelos de computação baseados em sistemas de qubits, qudits e qudits em sistemas representação redundantes.

No capítulo 1 apresenta-se, de uma forma sucinta e incompleta, uma introdução à Computação Quântica. Recorre-se sobretudo a exemplos para salientar as propriedades de paralelismo exponencial e entrelaçamento de estados presentes neste modelo de computação, os quais constituem os ingredientes base para o desenvolvimento de algoritmos quânticos.

No capítulo 2 estabelecem-se as noções fundamentais de um modelo de Computação Quântica generalizado, formalizando-se os conceitos de registo, medição, circuito, realização de operadores e reconhecimento de linguagens por circuitos.

O modelo geral proposto concretiza-se no capítulo 3, onde se estuda o problema da adição de números, representados por sequências de dígitos, em sistemas de representação redundantes. Tendo por bases dois algoritmos clássicos de adição originalmente descritos por Parhami [44], constroem-se duas classes de circuitos quânticos com profundidade constante e tamanho linear para a adição de dois números em sistemas redundantes. De uma forma unificada, estabelecem-se ainda condições necessárias e suficientes para a aplicação de um algoritmo

de adição de um número polinomial de números, sem propagação de dígitos de transporte. Relacionando estes resultados, com os trabalho de Cotofana e Vassiliadis [11, 12] na área de circuitos clássicos em Redes Neuronais e com os resultados de Høyer e Špalek [29][28] justifica-se a possibilidade de construir circuitos quânticos com profundidade constante para aproximar a soma de um número polinomial de números.

No capítulo 4 trata-se o problema da simulação de algoritmos quânticos em computadores clássicos. Apresentam-se as características únicas do *Simulador Simbólico de Computação Quântica*, valioso auxiliar na análise e desenvolvimento dos algoritmos de aritmética apresentados no capítulo 3. Analisam-se, a título exemplificativo, os resultados obtidos na simulação do algoritmo de Grover.

Tópicos de Computação Quântica $\langle \mathbf{1}|$

Neste primeiro capítulo, apresenta-se uma breve introdução à Computação Quântica. A selecção de tópicos pautou-se por salientar duas características essenciais da computação em sistemas quânticos: paralelismo exponencial e entrelaçamento. Com o propósito subjacente de introduzir a notação de Dirac, discutem-se os conceitos de sistema de qubits bem como a dinâmica e evolução em sistemas quânticos.

No apêndice A encontra-se uma compilação de alguns conceitos e definições básicas de Álgebra Linear referidos pela primeira vez neste capítulo.

De uma forma informal referem-se ainda as noções de portas e circuitos quânticos, exemplificados com o algoritmo de Deutsch-Jozsa. Para uma exposição completa dos tópicos aqui descritos, bem como de muitos outros omitidos, recomendam-se os textos de Nielsen e Chuang [39] ou Kitaev et al. [33].

1.1 Os bits quânticos

A unidade de informação quântica denomina-se *qubit*. Contrariamente ao *bit clássico*, conhecido por *bit de Shannon*, um qubit permite, em certo sentido, representar em simultâneo os valores 0 e 1.

Um exemplo de uma possível realização física de um qubit provém dos possíveis estados de polarização de um fotão: polarização vertical representada por $|\updownarrow\rangle$, polarização horizontal representada por $|\leftrightarrow\rangle$ ou uma sobreposição destes dois estados. Uma outra realização física de um qubit é dada por uma partícula de spin $\frac{1}{2}$, a qual se pode encontrar num estado de spin

para cima, estado esse representado por $|1\rangle$, num estado de spin para baixo, representado por $|0\rangle$, ou ainda numa sobreposição dos estados $|0\rangle$ e $|1\rangle$.

Independente de uma concretização física específica, considera-se um qubit como um modelo de um sistema quântico cujos possíveis estados são representáveis por certos elementos de um espaço de Hilbert de dimensão 2.

Os elementos de um espaço de Hilbert $\mathcal{H}$ denominam-se *vectores ket* ou simplesmente *kets*, representados segundo Dirac por $|\psi\rangle$, $|\phi\rangle$, etc.

Os elementos do espaço dual, $\mathcal{H}^\dagger$, de um espaço de Hilbert $\mathcal{H}$ denominam-se *vectores bra* ou simplesmente *bras* e denotam-se por $\langle\psi|$, $\langle\phi|$, etc.

Para um *bra* $\langle\phi|$ e um *ket* $|\psi\rangle$ o número complexo $\langle\phi|\,(|\psi\rangle)$, resultado da acção do funcional $\langle\phi|$ sobre $|\psi\rangle$, denota-se simplesmente por $\langle\phi|\psi\rangle$ e denomina-se um *braket*.

Exemplo 1.1. Polarização da Luz

Considere-se uma representação dos estados de polarização de um fotão por kets de um espaço de Hilbert, $\mathcal{H}$, de dimensão 2. Uma possível base ortonormada de $\mathcal{H}$ é constituída pelos kets $|\circlearrowleft\rangle$ e $|\circlearrowright\rangle$ os quais representam os dois sentidos possíveis da polarização circular do fotão. Uma outra base é constituída pelos kets $|\updownarrow\rangle$ e $|\leftrightarrow\rangle$ os quais representam, respectivamente, polarização vertical e polarização horizontal. Uma terceira possibilidade é dada pelos kets $|\nearrow\rangle$ e $|\searrow\rangle$ que representam, respectivamente, polarizações segundo os ângulos $\theta = \frac{\pi}{4}$ e $\theta = -\frac{\pi}{4}$. É claro que duas quaisquer bases estão relacionadas por intermédio de uma transformação linear[1]. A figura 1.1 sintetiza as relações entre as três bases anteriormente referidas.

Em termos da base $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ estes kets apresentam a seguinte forma vectorial:

$$|\updownarrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |\nearrow\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad |\circlearrowright\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$$

$$|\leftrightarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix} \qquad |\searrow\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \qquad |\circlearrowleft\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$$

Os estados de um sistema quântico correspondem a kets num certo espaço de Hilbert. Dois kets representam o mesmo estado se diferem apenas por um factor multiplicativo complexo.

[1] No caso de bases ortonormadas a transformação preserva o produto interno.

$$|\nearrow\rangle = \tfrac{1}{\sqrt{2}}\big(|\updownarrow\rangle + |\leftrightarrow\rangle\big) \qquad |\searrow\rangle = \tfrac{1}{\sqrt{2}}\big(|\updownarrow\rangle - |\leftrightarrow\rangle\big)$$
$$|\nearrow\rangle = \tfrac{1+i}{2}\,|\circlearrowright\rangle + \tfrac{1-i}{2}\,|\circlearrowleft\rangle \qquad |\searrow\rangle = \tfrac{1-i}{2}\,|\circlearrowright\rangle + \tfrac{1+i}{2}\,|\circlearrowleft\rangle$$
$$|\updownarrow\rangle = \tfrac{1}{\sqrt{2}}\big(|\nearrow\rangle + |\searrow\rangle\big) \qquad |\leftrightarrow\rangle = \tfrac{1}{\sqrt{2}}\big(|\nearrow\rangle - |\searrow\rangle\big)$$
$$|\updownarrow\rangle = \tfrac{1}{\sqrt{2}}\big(|\circlearrowright\rangle + |\circlearrowleft\rangle\big) \qquad |\leftrightarrow\rangle = \tfrac{i}{\sqrt{2}}\big(|\circlearrowright\rangle - |\circlearrowleft\rangle\big)$$
$$|\circlearrowright\rangle = \tfrac{1}{\sqrt{2}}\big(|\updownarrow\rangle - i\,|\leftrightarrow\rangle\big) \qquad |\circlearrowleft\rangle = \tfrac{1}{\sqrt{2}}\big(|\updownarrow\rangle + i\,|\leftrightarrow\rangle\big)$$
$$|\circlearrowright\rangle = \tfrac{1-i}{2}\,|\nearrow\rangle + \tfrac{1+i}{2}\,|\searrow\rangle \qquad |\circlearrowleft\rangle = \tfrac{1+i}{2}\,|\nearrow\rangle + \tfrac{1-i}{2}\,|\searrow\rangle$$

Figura 1.1: Relação entre três possíveis bases de polarização de um fotão

Mais precisamente, $|\phi\rangle$ e $|\psi\rangle$ representam o mesmo estado quântico se e só se existe um escalar não nulo $\alpha \in \mathbb{C}$ tal que $|\phi\rangle = \alpha\,|\psi\rangle$. Uma vez que um estado é representado por um ket a menos de um factor multiplicativo, identificam-se os estados com kets normalizados, i.e., kets $|\phi\rangle$ tais que $\langle\phi|\phi\rangle = 1$ ou seja $\| \, |\phi\rangle \, \| = 1$.

Desta forma é possível atribuir um caracter probabilístico aos coeficientes complexos, denominados amplitudes, na representação de um ket normalizado em termos de uma combinação linear complexa de vectores de uma base ortonormada. O quadrado do módulo de cada amplitude corresponde à probabilidade de observar o estado base ao qual está associada.

Exemplo 1.2. Considere-se a base ortonormada de um espaço de Hilbert de dimensão 2 constituída pelos kets $|0\rangle$ e $|1\rangle$, naturalmente associados aos dígitos binários 0 e 1. Seja $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ o estado de um qubit, com $|\alpha|^2 + |\beta|^2 = 1$. Nestas condições, a probabilidade de observar o bit 0 é $|\alpha|^2$ e a probabilidade de observar o bit 1 é $|\beta|^2$.

1.2 Sistemas de qubits

Considere-se um sistema constituído por dois bits clássicos. Os quatro possíveis estados do sistema são obviamente 00, 01, 10 e 11. De modo análogo um sistema de dois bits quânticos possui quatro estados base denotados por $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Mas em geral o estado do sistema de dois qubits é uma sobreposição desses estados, atribuindo a cada um deles uma

amplitude complexa. Mais precisamente, é um ket da forma

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\ .$$

O espaço de estados subjacente a um sistema de dois qubits tem portanto dimensão 4 e é dado pelo produto tensorial dos espaços de Hilbert associados a cada um dos qubits do sistema.

Se $|\phi\rangle$ e $|\psi\rangle$ são, respectivamente, kets dos espaços de Hilbert $\mathcal{H}_1$ e $\mathcal{H}_2$ então o seu produto tensorial é denotado por $|\phi\rangle \otimes |\psi\rangle$ ou simplesmente $|\phi\rangle\,|\psi\rangle$.

Exemplo 1.3. Considere-se um registo de dois qubits, i.e., um qualquer sistema quântico constituído por dois qubits. Sejam $\mathcal{H}_1$ e $\mathcal{H}_2$ os espaços de Hilbert subjacentes a cada um dos qubits, cada espaço de dimensão 2, com as bases $\{|0_1\rangle, |1_1\rangle\}$ e $\{|0_2\rangle, |1_2\rangle\}$ respectivamente. Em termos destas bases constrói-se uma base para o espaço produto tensorial $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$|0\rangle \equiv |00\rangle \equiv |0_1\rangle\,|0_2\rangle \equiv |0_1\rangle \otimes |0_2\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix}^{\intercal}$$

$$|1\rangle \equiv |01\rangle \equiv |0_1\rangle\,|1_2\rangle \equiv |0_1\rangle \otimes |1_2\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix}^{\intercal}$$

$$|2\rangle \equiv |10\rangle \equiv |1_1\rangle\,|0_2\rangle \equiv |1_1\rangle \otimes |0_2\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0 & 0 & 1 & 0\end{pmatrix}^{\intercal}$$

$$|3\rangle \equiv |11\rangle \equiv |1_1\rangle\,|1_2\rangle \equiv |1_1\rangle \otimes |1_2\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0 & 0 & 0 & 1\end{pmatrix}^{\intercal}$$

Considerem-se dois sistemas quânticos preparados nos estados $|\psi\rangle$ e $|\phi\rangle$ pertencentes a diferentes espaços de Hilbert, $\mathcal{H}_1$ e $\mathcal{H}_2$. Quando vistos como constituintes de um único

sistema quântico composto, o estado do sistema conjunto é o produto tensorial dos estados de cada um dos sistemas, $|\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$.

No entanto existem kets no espaço $\mathcal{H}_1 \otimes \mathcal{H}_2$ não representáveis na forma anterior.

Diz-se que um sistema composto por n sistemas quânticos com espaços de Hilbert subjacentes $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ se encontra em *entrelaçamento quântico* se não é possível decompor o seu estado $|\psi\rangle \in \mathcal{H} = \bigotimes_{j=1}^{n} \mathcal{H}_j$ num produto tensorial da forma

$$|\psi\rangle = \bigotimes_{j=1}^{n} |\psi_j\rangle \ ,$$

com cada ket $|\psi_j\rangle$ no espaço $\mathcal{H}_j$. Nesse caso diz-se ainda que o estado do sistema é *entrelaçado*.

No exemplo 1.8 da secção 1.5 o estado $|\psi_1\rangle$ é entrelaçado.

Exemplo 1.4. Considere-se um espaço de Hilbert $\mathcal{H}$ de dimensão 2 com uma base $\{|0\rangle, |1\rangle\}$. Sejam $\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{n-1}$ espaços de Hilbert, cada um deles isomorfo a $\mathcal{H}$ e com as bases induzidas pelos isomorfismos: $\{|0\rangle_i, |1\rangle_i\}$, $i \in [0 \,..\, n-1]$.

Suponha-se que cada um dos qubits de um registo de n qubits é inicialmente preparado no estado

$$\frac{1}{\sqrt{2}} \left(|0_i\rangle + |1_i\rangle \right), \ i \in [0 \,..\, n-1] \ .$$

Então o estado do sistema quântico constituído pelos n qubits é o ket $|\psi\rangle$, no espaço produto tensorial $\mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \ldots \otimes \mathcal{H}_0$, idêntico a

$$\begin{aligned} |\psi\rangle &= \tfrac{1}{\sqrt{2}} \left(|0_{n-1}\rangle + |1_{n-1}\rangle \right) \otimes \tfrac{1}{\sqrt{2}} \left(|0_{n-2}\rangle + |1_{n-2}\rangle \right) \otimes \ldots \otimes \tfrac{1}{\sqrt{2}} \left(|0_0\rangle + |1_0\rangle \right) \\ &= \left(\tfrac{1}{\sqrt{2}} \right)^n \Big(|0_{n-1}\rangle \, |0_{n-2}\rangle \ldots |0_1\rangle \, |0_0\rangle \\ &\qquad + |0_{n-1}\rangle \, |0_{n-2}\rangle \ldots |0_1\rangle \, |1_0\rangle \\ &\qquad\quad + \ldots \\ &\qquad\quad + |1_{n-1}\rangle \, |1_{n-2}\rangle \ldots |1_1\rangle \, |1_0\rangle \Big) \, . \end{aligned}$$

Ao identificar os n espaços de Hilbert com $\mathcal{H}$, omitem-se os índices, e a expressão anterior é simplesmente

$$|\psi\rangle = \left(\tfrac{1}{\sqrt{2}} \right)^n \left(|00\ldots00\rangle + |00\ldots01\rangle + \ldots + |11\ldots11\rangle \right) \in \bigotimes_i \mathcal{H}_i = \mathcal{H}^{\otimes n} \, .$$

O estado do registo de n qubits é então uma sobreposição dos kets rotulados pelas sequências de n bits. Cada uma das sequências binárias $b_{n-1}b_{n-2}\ldots b_1b_0$ identifica-se naturalmente com o inteiro $b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+\ldots+b_12^1+b_02^0$. Assim, interpretando cada sequência como a representação binária de um inteiro, é possível escrever o estado do registo quântico na forma

$$|\psi\rangle = \left(\tfrac{1}{\sqrt{2}}\right)^n \left(|0\rangle + |1\rangle + |2\rangle + \ldots + |2^n-1\rangle\right).$$

Esta última expressão sugere que o registo contém uma sobreposição dos inteiros desde 0 a 2^n-1, um paralelismo massivo, o qual é realizável de forma eficiente (cf. capítulo 4 e apêndice B). Em contrapartida, uma única medição do registo destruirá completamente o paralelismo: o "mundo quântico" selecciona um e um só dos 2^n inteiros com probabilidade $\left|\left(\tfrac{1}{\sqrt{2}}\right)^n\right|^2 = \dfrac{1}{2^n}$. Note-se ainda que o estado $|\psi\rangle$ não é entrelaçado.

1.3 Observação de um sistema quântico

A acção de um operador linear $\mathbf{A}$ sobre um ket $|\psi\rangle$, $\mathbf{A}(|\psi\rangle)$, denota-se simplesmente por $\mathbf{A}\,|\psi\rangle$. Para dois kets $|\psi\rangle, |\phi\rangle$ num espaço de Hilbert $\mathcal{H}$, o *operador produto externo*, $|\psi\rangle\langle\phi|$, é um operador linear definido por $|\psi\rangle\langle\phi|\,|\eta\rangle = |\psi\rangle\,\langle\phi|\eta\rangle = \langle\phi|\eta\rangle\,|\psi\rangle$, para $|\eta\rangle \in \mathcal{H}$.

Um *observável* é uma propriedade de um sistema quântico que em princípio pode ser medida. Em von Neumann [53] consideram-se medições projectivas ortogonais, obtidas por decomposição espectral de observáveis. Veja-se a definição e algumas propriedades básicas no apêndice A.

Exemplo 1.5. Sejam $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ uma base ortonormada de um espaço de Hilbert $\mathcal{H}$ e $\mathbf{A}$ o observável representado naquela base pela matriz

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 1 \\ i & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Este observável é degenerado, com 2 valores próprios $\lambda_0 = +1$ e $\lambda_1 = -1$. Uma base ortonormada para o espaço próprio $\mathcal{P}_{\lambda_0}$ é constituída pelos kets

$$|+1,0\rangle = \frac{1}{\sqrt{2}}(-i\,|0\rangle + |2\rangle) = \frac{1}{\sqrt{2}}(-i\ 0\ 1\ 0)^\intercal \quad \text{e} \quad |+1,1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |3\rangle) = \frac{1}{\sqrt{2}}(0\ 1\ 0\ 1)^\intercal.$$

De igual modo, uma base ortonormada para o espaço próprio $\mathcal{P}_{\lambda_1}$ é

$$|-1,0\rangle = \frac{1}{\sqrt{2}}(i\,|0\rangle + |2\rangle) = \frac{1}{\sqrt{2}}(i\ 0\ 1\ 0)^\intercal \quad \text{e} \quad |-1,1\rangle = \frac{1}{\sqrt{2}}(-\,|1\rangle + |3\rangle) = \frac{1}{\sqrt{2}}(0\ -1\ 0\ 1)^\intercal.$$

A decomposição espectral do observável $\mathbf{A}$ é assim

$$\mathbf{A} = \lambda_0 \mathbf{P}_{\lambda_0} + \lambda_1 \mathbf{P}_{\lambda_1} = (|+1,0\rangle\langle+1,0| + |+1,1\rangle\langle+1,1|) - (|-1,0\rangle\langle-1,0| + |-1,1\rangle\langle-1,1|)$$

e a sua representação matricial em termos da base $|+1,0\rangle\,,\ |+1,1\rangle\,,\ |-1,0\rangle\,,\ |-1,1\rangle$ é a matriz diagonal

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Note-se ainda que $\mathbf{P}_{\lambda_0}$ e $\mathbf{P}_{\lambda_1}$ constituem um *conjunto completo de projectores ortogonais*, isto é, $\mathbf{P}_{\lambda_0} + \mathbf{P}_{\lambda_1} = \big(|+1,0\rangle\langle+1,0| + |+1,1\rangle\langle+1,1|\big) + \big(|-1,0\rangle\langle-1,0| + |-1,1\rangle\langle-1,1|\big) = \mathbf{I}$.

A *medição de um observável* $\mathbf{A}$ de um sistema quântico num estado $|\psi\rangle$ tem como resultado um valor próprio de $\mathbf{A}$, λ_i, com probabilidade

$$\text{prob}(\lambda_i) = \|\mathbf{P}_{\lambda_i}\,|\psi\rangle\|^2 = \langle\psi|\,\mathbf{P}_{\lambda_i}\,|\psi\rangle\ .$$

Além disso o estado do sistema quântico após a medição é o elemento do espaço próprio $\mathcal{P}_{\lambda_i}$ dado por

$$\frac{\mathbf{P}_{\lambda_i}\,|\psi\rangle}{\sqrt{\langle\psi|\,\mathbf{P}_{\lambda_i}\,|\psi\rangle}}\,.$$

Como se ilustra na figura 1.2, se o resultado de uma medição do estado do sistema quântico for λ_i com probabilidade $\langle\psi|\,\mathbf{P}_{\lambda_i}\,|\psi\rangle$ então uma segunda medição com o mesmo observável

$$|\psi\rangle = \sum_i \mathbf{P}_{\lambda_i} |\psi\rangle \quad \overset{1^{\text{a}}\text{ medição}}{\longrightarrow} \quad \frac{\mathbf{P}_{\lambda_i}|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_{\lambda_i}|\psi\rangle}} \quad \overset{2^{\text{a}}\text{ medição}}{\longrightarrow} \quad \frac{\mathbf{P}_{\lambda_i}|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_{\lambda_i}|\psi\rangle}}$$
$$\text{prob} = \langle\psi| \mathbf{P}_{\lambda_i} |\psi\rangle \qquad \text{prob} = 1$$

Figura 1.2: Medição de um observável de um sistema quântico.

já não possui carácter probabilístico: o resultado é o mesmo valor próprio λ_i e o estado do sistema mantém-se idêntico a $\frac{\mathbf{P}_{\lambda_i}|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_{\lambda_i}|\psi\rangle}}$.

Exemplo 1.6. Sejam $\mathcal{H}$ o espaço de Hilbert e $\mathbf{A}$ o observável definidos no exemplo 1.5 e considere-se um sistema quântico preparado no estado

$$|\psi\rangle = \tfrac{i}{\sqrt{3}}|0\rangle - \tfrac{1}{\sqrt{3}}|2\rangle + \tfrac{1}{\sqrt{3}}|3\rangle = \tfrac{1}{\sqrt{3}}(i, 0, -1, 1)^{\intercal}.$$

Na base $|+1,0\rangle$, $|+1,1\rangle$, $|-1,0\rangle$, $|-1,1\rangle$, o estado $|\psi\rangle$ é idêntico a

$$|\psi\rangle = -\tfrac{\sqrt{2}}{\sqrt{3}}|1,0\rangle + \tfrac{\sqrt{2}}{2\sqrt{3}}\left(|1,1\rangle + |-1,1\rangle\right).$$

A medição do sistema quântico relativamente ao observável $\mathbf{A}$ tem como resultado

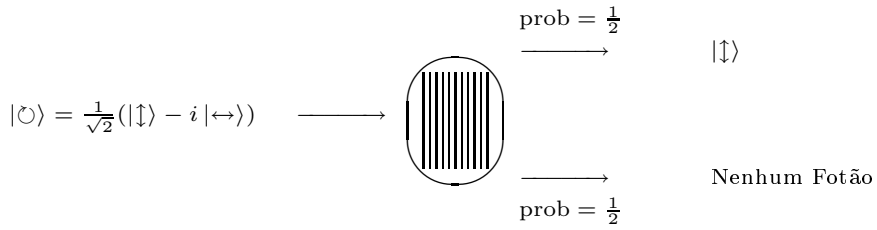
- o valor próprio $\lambda_0 = +1$ com probabilidade $\frac{5}{6}$ e o estado do sistema passa a ser $\frac{1}{\sqrt{5}}\left(-2|1,0\rangle + |1,1\rangle\right)$. Este estado é idêntico a

$$\tfrac{2i}{\sqrt{10}}|0\rangle + \tfrac{1}{\sqrt{10}}|1\rangle - \tfrac{2}{\sqrt{10}}|2\rangle + \tfrac{1}{\sqrt{10}}|3\rangle\ .$$

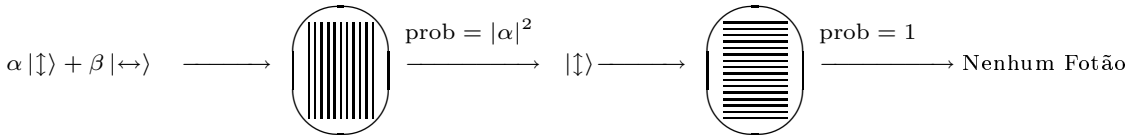
- ou o valor próprio $\lambda_1 = -1$ com probabilidade $\frac{1}{6}$ e, neste caso, o estado do sistema passa a ser $|-1,1\rangle = \frac{1}{\sqrt{2}}(-|1\rangle + |3\rangle)$.

Recorrendo a um outro exemplo, comum na literatura, ilustram-se estas propriedades da Mecânica Quântica, no mínimo pouco intuitivas numa perspectiva clássica, todavia experimentalmente confirmadas.

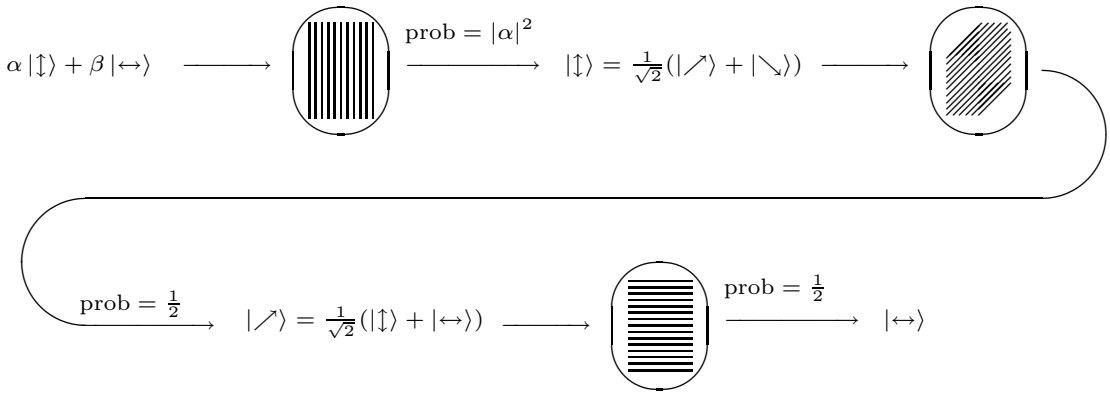
Exemplo 1.7. Polarização da Luz. Tendo em conta as relações apresentadas na figura 1.1 ilustra-se em seguida uma experiência em que um fotão polarizado circularmente para a direita incide num filtro de polarização vertical, o qual mede o observável $|\updownarrow\rangle\langle\updownarrow|$.



Na experiência seguinte colocou-se um filtro de polarização horizontal, o qual mede o observável $|\leftrightarrow\rangle\langle\leftrightarrow|$, a seguir a um filtro de polarização vertical. A probabilidade de encontrar um qualquer fotão no estado $\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$, em que $|\alpha|^2 + |\beta|^2 = 1$, a seguir ao último filtro é nula.



Obtém-se um resultado inesperado quando se coloca um filtro diagonalmente polarizado, o qual mede o observável $|\nearrow\rangle\langle\nearrow|$, entre os dois filtros da experiência anterior. De facto, a probabilidade de observar um fotão a seguir ao último filtro não é nula, como se ilustra em seguida.



1.4 O Princípio da Incerteza de Heisenberg

O valor esperado de uma medição de um estado $|\psi\rangle$ por um observável $\mathbf{A}$ é

$$\langle \mathbf{A} \rangle = \langle \psi |\, \mathbf{A}\, |\psi\rangle \ .$$

Demonstra-se em seguida esta propriedade, com o objectivo de ilustrar a notação de Dirac.

Sejam $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ os valores próprios distintos do observável $\mathbf{A}$ e $\mathbf{P}_{\lambda_0}, \mathbf{P}_{\lambda_1}, \ldots, \mathbf{P}_{\lambda_{n-1}}$ os respectivos projectores. Pelo teorema da decomposição espectral, $\mathbf{A} = \sum_{j=0}^{n-1} \lambda_j \mathbf{P}_{\lambda_j}$ e o valor próprio observado esperado é assim dado por

$$\langle \mathbf{A} \rangle = \sum_{j=0}^{n-1} \lambda_j \, \mathrm{prob}(\lambda_j).$$

Mas $\mathrm{prob}(\lambda_j) = \langle \psi | \, \mathbf{P}_{\lambda_j} \, | \psi \rangle$. Logo

$$\langle \mathbf{A} \rangle = \sum_{j=0}^{n-1} \lambda_j \, \langle \psi | \, \mathbf{P}_{\lambda_j} \, | \psi \rangle = \langle \psi | \sum_{j=0}^{n-1} \mathbf{P}_{\lambda_j} \, | \psi \rangle = \langle \psi | \, \mathbf{A} \, | \psi \rangle \ .$$

q.e.d.

A incerteza envolvida no processo de medição de um observável $\mathbf{A}$ define-se como o desvio padrão dos valores próprios observados,

$$\sqrt{\left\langle (\Delta \mathbf{A})^2 \right\rangle},$$

em que $\Delta \mathbf{A} = \mathbf{A} - \langle \mathbf{A} \rangle$.

Dois observáveis $\mathbf{A}$ e $\mathbf{B}$ dizem-se *compatíveis* se *comutam* entre si, isto é, se $\mathbf{AB} = \mathbf{BA}$. Caso contrário, dizem-se *incompatíveis*.

O *comutador* de dois operadores lineares $\mathbf{A}$ e $\mathbf{B}$ define-se por

$$[\mathbf{A}, \mathbf{B}] = \mathbf{AB} - \mathbf{BA}.$$

Assim, dois observáveis $\mathbf{A}$ e $\mathbf{B}$ são compatíveis se e só se $[\mathbf{A}, \mathbf{B}] = 0$.

A desigualdade de Cauchy-Schwarz permite demonstrar a designada relação de Robertson-Schrödinger,

$$\left\langle (\Delta \mathbf{A})^2 \right\rangle \left\langle (\Delta \mathbf{B})^2 \right\rangle \geq \frac{1}{4} \left| \langle [\mathbf{A}, \mathbf{B}] \rangle \right|^2 \ .$$

Substituindo nesta última expressão $\mathbf{A}$ por $\mathbf{A} - \langle \mathbf{A} \rangle$ e $\mathbf{B}$ por $\mathbf{B} - \langle \mathbf{B} \rangle$ obtém-se o princípio da incerteza de Heisenberg na forma

$$\Delta \mathbf{A} \cdot \Delta \mathbf{B} \geq \frac{1}{2} \left| \langle [\mathbf{A}, \mathbf{B}] \rangle \right| \ .$$

Salienta-se que estas propriedades devem ser interpretadas no contexto da Mecânica Estatística e não como resultado de duas únicas observações consecutivas de um mesmo sistema quântico pelos observáveis $\mathbf{A}$ e $\mathbf{B}$.

1.5 Dinâmica de sistemas quânticos fechados

Os *operadores unitários* são fundamentais em mecânica quântica nomeadamente porque:

- Os sistemas quânticos fechados evoluem somente por acção de transformações unitárias.
- As transformações unitárias preservam as probabilidades quânticas.

A análise do comportamento dinâmico de sistemas quânticos abertos é muito mais complexa e não é abordada neste trabalho.

Seja $|\psi(t)\rangle$ o estado como função do tempo t de um sistema mecânico quântico fechado. O comportamento dinâmico desse sistema é determinado pela equação de Schrödinger

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = \mathbf{H}|\psi(t)\rangle\,,$$

em que $\hbar$ denota a constante de Planck dividida por 2π, e $\mathbf{H}$ é o Hamiltoniano. É possível escrever esta equação na forma

$$\frac{\partial}{\partial t}\mathbf{U}(t) = -\frac{i}{\hbar}\mathbf{H}(t)\mathbf{U}(t)\,,$$

em que $|\psi(t)\rangle = \mathbf{U}(t)|\psi(0)\rangle$ e a solução é dada por

$$\mathbf{U}(t) = \lim_{n\to\infty} e^{-\frac{i}{\hbar}\mathbf{H}(n\frac{t}{n})\frac{t}{n}} \cdot e^{-\frac{i}{\hbar}\mathbf{H}((n-1)\frac{t}{n})\frac{t}{n}} \cdot \ldots \cdot e^{-\frac{i}{\hbar}\mathbf{H}(1\frac{t}{n})\frac{t}{n}} \cdot e^{-\frac{i}{\hbar}\mathbf{H}(0\frac{t}{n})\frac{t}{n}}$$

Quando o Hamiltoniano é independente do tempo, $\mathbf{H}(t) = \mathbf{H}$, a fórmula anterior simplifica-se para $\mathbf{U}(t) = e^{-\frac{i}{\hbar}\mathbf{H}t}$.

Exemplo 1.8. Considere-se o estado de um um registo de 2 qubits no instante $t = 0$,

$$|\psi_0\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}.$$

Suponha-se que o comportamento dinâmico do registo entre os instantes $t = 0$ e $t = 1$ é determinado por um Hamiltoniano constante, $\mathbf{H}$, definido em termos da base $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ por

$$\mathbf{H} = \frac{\pi\hbar}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} .$$

Pela equação de Schrödinger, o Hamiltoniano $\mathbf{H}$ determina a transformação unitária

$$\mathbf{U} = e^{-\frac{i}{\hbar}\mathbf{H}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 3| + |3\rangle\langle 2| \ .$$

O estado inicial do registo evolui por acção de $\mathbf{U}$ de tal modo que no instante $t = 1$ o estado do sistema é $|\psi_1\rangle = \mathbf{U}\,|\psi_0\rangle$. Explicitamente,

$$|\psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle - |3\rangle\big) \, .$$

O estado resultante, denominado um estado EPR em homenagem a Einstein, Podolsky e Rosen, possui a propriedade notável de ser impossível escrevê-lo como um produto tensorial de dois estados, cada estado associado a um dos qubits do sistema. Num certo sentido, os qubits perderam a sua individualidade. Por exemplo, a medição de apenas um dos qubits permite conhecer o estado do segundo qubit do sistema.

1.6 Portas e circuitos quânticos

São sobejamente conhecidas diversas técnicas gerais de decomposição de operadores lineares como produto de "operadores mais simples".

No contexto da Computação Quântica mostra-se que existem conjuntos universais de operadores unitários, designados bases de operadores unitários, tais que qualquer operador unitário se pode escrever como produto de operadores dessa base. Para além disso, estabelecendo uma definição apropriada de distância entre operadores, mostra-se que existem conjuntos finitos de operadores unitários que permitem aproximar qualquer operador unitário usando apenas operadores dessa base.

Dada a sua importância prática bem como ao nível da complexidade computacional este assunto tem sido tratado por diversos autores, veja-se por exemplo Kitaev et al. [33], pág. 188–200 ou, para uma abordagem mais formal, Brylinski e Brylinski [9].

O mais simples exemplo não trivial (diferente da identidade $\mathbf{I}$) de uma porta quântica sobre um qubit é sem dúvida o análogo quântico da porta clássica NOT, denotada por $\mathbf{X}$ e definida relativamente à base $\{|0\rangle, |1\rangle\}$ de um espaço de Hilbert de dimensão 2 pela matriz

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Conhecido também por operador de negação ou porta **NOT**, $\mathbf{X}$ satisfaz $\mathbf{X}|0\rangle = |1\rangle$ e $\mathbf{X}|1\rangle = |0\rangle$.

Um outro exemplo fundamental de uma porta quântica de um qubit, por permitir criar estados que são sobreposições uniformes de estados base, é a porta de Hadamard, $\mathbf{H}$. Define-se relativamente à base $\{|0\rangle, |1\rangle\}$ por

$$\mathbf{H}|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^i |1\rangle\right),\ i = 0, 1.$$

A figura 1.3 ilustra a acção de $\mathbf{H}$ sobre um qubit inicialmente no estado $|0\rangle$.

Uma decomposição de um operador unitário num produto tensorial de operadores permite considerar uma realização desse operador em paralelo, pelas portas quânticas associadas aos

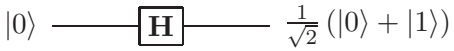


Figura 1.3: A porta quântica de Hadamard.

factores da decomposição. Reciprocamente, a aplicação em paralelo de um conjunto de portas quânticas é formalizada pelo produto tensorial dos operadores subjacentes a essas portas.

Por exemplo, o estado do registo de n qubits considerado no exemplo 1.4 obtém-se por aplicação em paralelo de n portas de Hadamard, $\mathbf{H} \otimes \cdots \otimes \mathbf{H}$.

No entanto, existem operadores unitários que não se podem escrever na forma de um produto tensorial de operadores, cada um deles associado a um dos qubits do sistema. Exemplo disso é a porta **CNOT**, a qual generaliza a porta clássica XOR, definida relativamente à base $\{|i\rangle \otimes |j\rangle : i, j = 0, 1\}$ por

$$\mathbf{CNOT}\,|i\rangle\,|j\rangle = |i\rangle\,|i \oplus j\rangle \ ,$$

onde $\oplus$ denota adição módulo 2. A figura seguinte ilustra a acção deste operador.

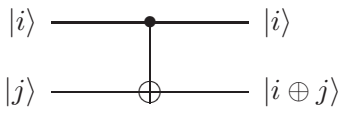


Figura 1.4: Acção da porta **CNOT**.

Combinando sequencialmente e ou em paralelo um número suficiente de portas quânticas, é possível realizar operadores unitários com complexidade crescente. A noção de *circuito quântico* corresponde a um algoritmo para realizar um operador unitário a partir de um pré-determinado conjunto de portas elementares. É ainda usual representar graficamente os circuitos quânticos numa grelha rectangular. As linhas horizontais, designadas fios quânticos, representam os qubits do sistema. Em pontos específicos ao longo da grelha, inscrevem-se pequenas caixas ou conectam-se verticalmente fios quânticos. Cada caixa ou ligação vertical representa uma porta quântica. Em cada diagrama de um circuito considera-se ainda uma linha temporal orientada da esquerda para a direita a qual define a ordem de aplicação das

portas quânticas.

Por exemplo, se o estado inicial de um qubit for $|0\rangle$ então pela acção sequencial das portas quânticas $\mathbf{X}$ e $\mathbf{H}$, o estado do qubit altera-se para $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. O diagrama do circuito quântico correspondente ilustra-se na figura 1.5.

Figura 1.5: Circuito quântico para o operador $\mathbf{H} \cdot \mathbf{X}$.

Considere-se ainda o exemplo 1.8 e observe-se que a matriz unitária $\mathbf{U}$ ali considerada não é mais do que a matriz do operador **CNOT**. Então um circuito quântico que descreve a evolução daquele sistema é o da figura seguinte.

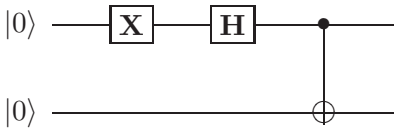


Figura 1.6: Um circuito para obter um estado EPR.

Mostra-se ser possível transformar qualquer circuito booleano clássico para avaliar uma função booleana $f : \{0,1\}^n \to \{0,1\}^m$ num circuito clássico equivalente que utiliza apenas portas reversíveis. A partir deste constrói-se um circuito quântico para implementar a função f, [33, págs. 60–65].

Assim, considere-se $g : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$, a versão reversível de f definida por $g(i,j) = (i, j \oplus f(i))$ onde $\oplus$ denota a adição bit a bit módulo 2. Note-se que a função g é uma permutação de $\{0,1\}^{n+m}$ à qual corresponde naturalmente o operador unitário $\mathbf{U}_f$ num espaço de Hilbert de dimensão 2^{m+n} definido por

$$\mathbf{U}_f |i\rangle |j\rangle = |i\rangle |j \oplus f(i)\rangle \ ,$$

para $i \in \{0,1\}^n$ e $j \in \{0,1\}^m$.

1.7 Algoritmos quânticos

Um dos primeiros e mais simples algoritmos que ilustra a forma como a Computação Quântica explora as propriedades da Mecânica Quântica é sem dúvida o algoritmo de Deutsch [15], representado na figura 1.7.

Seja $f : \{0,1\} \to \{0,1\}$ uma função booleana. Para determinar se f é ou não uma função constante parece claro, no contexto clássico, ser necessário avaliar a função em $f(0)$ e $f(1)$. Como se verifica em seguida, o circuito de Deutsch permite aferir a mesma propriedade sobre a função f utilizando uma única vez a porta quântica $\mathbf{U}_f$.

Considerem-se dois qubits inicialmente nos estados $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. A preparação destes estados realiza-se aplicando em paralelo portas de Hadamard. Desta forma o estado inicial do sistema é simplesmente o produto tensorial dos estados

$$|\psi_1\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)\,.$$

Simples manipulações algébricas permitem verificar que, para $i \in \{0,1\}$, a acção da porta $\mathbf{U}_f$ sobre um estado da forma $\frac{1}{\sqrt{2}}\,|i\rangle\,(|0\rangle - |1\rangle)$ resulta em $\frac{1}{\sqrt{2}}(-1)^{f(i)}\,|i\rangle\,(|0\rangle - |1\rangle)$. Assim

$$|\psi_2\rangle = \mathbf{U}_f\,|\psi_1\rangle = \begin{cases} \pm\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \text{ se } f(0) = f(1) \\ \pm\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \text{ se } f(0) \neq f(1)\,. \end{cases}$$

Ao aplicar a porta de Hadamard ao primeiro qubit do sistema, o estado resultante é

$$|\psi_3\rangle = (\mathbf{H} \otimes \mathbf{I})\,|\psi_2\rangle = \begin{cases} \pm\frac{1}{2}\,|0\rangle \otimes (|0\rangle - |1\rangle) \text{ se } f(0) = f(1) \\ \pm\frac{1}{2}\,|1\rangle \otimes (|0\rangle - |1\rangle) \text{ se } f(0) \neq f(1)\,. \end{cases}$$

Logo a medição final do estado do primeiro qubit do sistema, denotada por  , permite determinar se f é ou não constante.

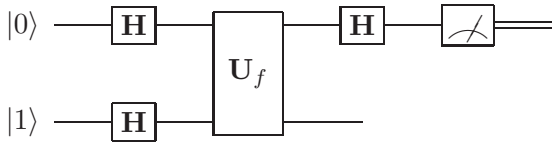


Figura 1.7: Circuito quântico para o algoritmo de Deutsch.

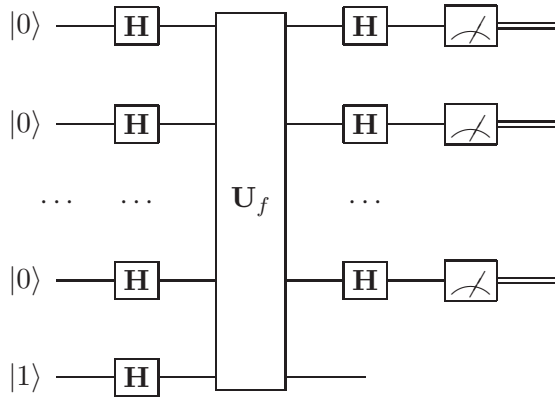


Figura 1.8: Circuito quântico para o algoritmo de Deutsch-Jozsa.

Talvez se possam colocar algumas objecções quanto a comparar a eficiência da avaliação clássica de uma função f em dois pontos contra uma única utilização da porta quântica $\mathbf{U}_f$. No entanto estas dissipam-se completamente quando se considera uma extensão do algoritmo Deutsch, o algoritmo de Deutsch-Jozsa [17].

Neste algoritmo, considera-se uma função booleana $f : \{0,1\}^n \to \{0,1\}$ juntamente com uma promessa de que esta é constante ou equilibrada (i.e., toma tantos valores 0 como 1). Qualquer algoritmo clássico determinista para decidir esta propriedade de f necessita de avaliar a função em $2^{n-1}+1$ pontos de $\{0,1\}^n$. No entanto o circuito quântico representado na figura 1.8 permite resolver o problema usando uma única vez a porta $\mathbf{U}_f$. Uma análise semelhante à realizada para o algoritmo de Deutsch permite concluir que a observação de pelo menos um bit 1 como resultado da medição do estado final dos n primeiros qubits do sistema indica que a função é equilibrada (se os n bits observados são 0 então a função é constante).

Em 1994, Simon [50, 51] apresenta um avanço relativamente ao algoritmo de Deutsch-Jozsa. O algoritmo de Simon permite testar a periodicidade das representações binárias de uma função $f : \{0,1\}^n \to \{0,1\}^m$.

Substituindo as portas de Hadamard no circuito de Simon por uma transformada de Fourier quântica, Peter Shor obtém em 1994 um algoritmo quântico para resolver em tempo polinomial o problema da factorização de números inteiros em primos. Este resultado tem enorme importância tanto na área da criptografia bem como ao nível da complexidade computacional, por não se conhecerem algoritmos clássicos, quer deterministas quer probabilísticos,

para factorizar números inteiros. Os detalhes do algoritmo podem ser consultados nos trabalhos originais de Shor [48, 49] ou em Pereira e Rodrigues [46]. Todos estes algoritmos foram entretanto generalizados e unificados, sendo actualmente conhecidos por algoritmos quânticos para estimação de fase [31], [21], [1].

Numa outra vertente surge ainda o algoritmo quântico de Grover [27], discutido no capítulo 4, e generalizações posteriores conhecidas por algoritmos quânticos de amplificação de amplitudes [8], [30].

Circuitos Quânticos e Complexidade $\langle \mathbf{2}|$

As origens da Teoria da Complexidade no Modelo de Computação Quântica situam-se na década de 80 com os trabalhos pioneiros de Benioff [3, 4, 5]. Seguiu-se o desenvolvimento e formalização do modelo da Máquina de Turing Quântica por Deutsch [15], Bernstein e Vazirani [6].

Pela mesma altura Deutsch [16] propõe, em alternativa, o Modelo de Circuitos Quânticos posteriormente desenvolvido por Yao [55]. A equivalência entre estes modelos tem sido investigada por vários autores, entre outros Nishimura e Ozawa [41, 42, 43].

Entretanto, surge a ideia de um modelo de computação em sistemas quânticos nos quais a unidade de informação, o qudit, possui mais do que os dois níveis distintos permitidos pelo qubit [2],[13].

Não é de todo claro que os modelos de computação baseados em qubits sejam equivalentes a modelos baseados em qudits, muito menos em que sentido existirá uma tal equivalência. As dificuldades aumentam quando se pensa sistemas de computação com misturas de diferentes unidades de informação, designados sistemas híbridos [37].

Desde cedo se tornou evidente ser necessário enquadrar os algoritmos de Aritmética em Sistemas de Representação Redundantes, descritos no capítulo 3, sob um modelo formal que permitisse uma posterior análise comparativa com os métodos da Computação Quântica em sistema de qubits. Nesse sentido, propõe-se neste capítulo uma possível formalização de um modelo de Computação em Sistemas Quânticos Híbridos, o qual generaliza, por inclusão, os modelos baseados em sistemas de qubits, qudits e qudits para sistemas representação redundantes.

2.1 Registos quânticos

"*... quantum phenomena do not occur in a Hilbert space,*
they occur in a laboratory. "
Asher Peres

Subjacente a cada sistema quântico considera-se um espaço de Hilbert, o espaço de estados. Os possíveis estados de um sistema quântico são representados, seguindo Dirac, por *kets* $|\phi\rangle$, $|\psi\rangle$, etc. Nesta tese assume-se que todos os espaços têm dimensão finita.

Associado a cada sistema quântico considera-se ainda uma base ortonormada preferencial do espaço de Hilbert subjacente, a base computacional. Os estados de um sistema quântico são ainda identificados com os vectores de norma um do espaço de Hilbert subjacente. Assim, cada estado é representado por uma combinação linear, com coeficientes em $\mathbb{C}$, dos vectores da base computacional.

Para representar os vectores da base computacional de um sistema quântico recorre-se a uma linguagem Γ, cujo cardinal se denota por $|\Gamma|$.

Definição 2.1. O *espaço de estados* sobre uma linguagem Γ, $\mathcal{H}(\Gamma)$, é o espaço de Hilbert de dimensão $|\Gamma|$ gerado pela base ortonormada constituída pelos vectores $|s\rangle$, $s \in \Gamma$. Esta base denomina-se *base computacional*.

Definição 2.2. Seja Γ uma linguagem. Um Γ*–qudit* é um sistema quântico com um espaço de estados subjacente $\mathcal{H}(\Gamma)$.

Na definição anterior, a pertinente questão do que se entende por sistema quântico, embora fundamental de um ponto de vista tecnológico, não se aprofundada neste trabalho. Nota-se apenas que, na prática, cada Γ–qudit é realizado por um sistema físico concreto.

É possível (e adequado) prosseguir o desenvolvimento teórico de um Modelo de Computação Quântica de modo independente das concretizações específicas, actuais ou futuras, do objecto matemático qudit. Nesse sentido, é conveniente estabelecer um conjunto de princípios fundamentais que evitem o desfazamento do modelo relativamente à realidade física subjacente.

> **Postulado 1:** *Associado a um sistema físico isolado existe um espaço vectorial com produto interno, o espaço de estados. O sistema é completamente descrito por um vector de estado, um vector de norma um no espaço de estados do sistema.*

Assim, assume-se que o conteúdo matemático do objecto físico qudit é completamente capturado pela noção de estado.

Definição 2.3. Um *estado* de um Γ–qudit é um vector de norma um do espaço de estados subjacente $\mathcal{H}(\Gamma)$.

O estado de um Γ–qudit denota-se por um *ket*. Por exemplo, para $s \in \Gamma$, a expressão $|\psi\rangle = |s\rangle$ significa que o estado do qudit é $|s\rangle$. Da definição anterior decorre que a forma geral do estado de um Γ–qudit é uma combinação linear complexa dos *estados base*, i.e, dos elementos da base computacional, da forma

$$\begin{gathered} |\psi\rangle = \sum_{s\in\Gamma} \alpha_s \, |s\rangle, \\ \text{para } \alpha_s \in \mathbb{C}, s \in \Gamma \,, \end{gathered} \tag{2.1}$$

que satisfaça a condição de normalização

$$\sum_{s\in\Gamma} |\alpha_s|^2 = 1 \,. \tag{2.2}$$

Observação 2.1. A definição usual de qudit obtém-se das definições anteriores considerando $\Gamma = [0 \,..\, d-1]$ e denomina-se simplesmente d–qudit. A definição de qubit corresponde a $\Gamma = \{0, 1\}$.

Uma vez definidas as unidades básicas de informação, os Γ–qudits, é agora necessário formalizar o conceito de sistema de qudits. Nesse sentido, denomina-se *sistema quântico composto* um sistema quântico no qual se identificam vários subsistemas. Se se considerar cada qudit como um sistema quântico isolado então é possível considerar que os estados de uma colecção de qudits são tuplos de estados, cada um associado a um dos qudits do sistema. No entanto, nem todos os possíveis estados de um sistema quântico composto são caracterizáveis por sequências de estados associados aos subsistemas. Nesses casos diz-se que o sistema quântico se encontra num estado entrelaçado (*o todo é maior que a soma das partes*).

> **Postulado 2:** *O espaço de estados subjacente a um sistema quântico composto por vários subsistemas identifica-se com o produto tensorial dos espaços associados a cada um dos subsistemas.*

Na secção 2.3 ver-se-á que os elementos da linguagem Γ, bem como os respectivos estados base, estão intrinsecamente associados às quantidades possíveis de observar num sistema quântico. Parece lógico pensar-se que os valores observáveis num sistema quântico composto sejam tuplos de valores observáveis, cada valor associado a um subsistema. Este é o ponto de vista adoptado com o intuito de formalizar o conceito de estado de um sistema quântico composto.

Designa-se por *linguagem produto* de n linguagens $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ a linguagem dada pelo produto cartesiano

$$\Gamma = \Gamma_1 \Gamma_2 \cdots \Gamma_n \quad .$$

Diz-se neste caso que Γ tem comprimento n e escreve-se $\mathrm{comp}(\Gamma) = n$. Note-se que as palavras de uma linguagem produto têm todas o mesmo comprimento e são da forma $s_1 s_2 \ldots s_n \equiv (s_1, s_2, \ldots, s_n)$ para $s_1 \in \Gamma_1, s_2 \in \Gamma_2, \ldots, s_n \in \Gamma_n$.

Definição 2.4. Seja Γ uma linguagem produto. Um Γ–*qudit composto* é um sistema quântico com um espaço de estados subjacente $\mathcal{H}(\Gamma)$.

Pela definição anterior a base computacional do espaço de estados de um Γ–qudit composto é constituída por $|\Gamma|$ estados $|s_1 s_2 \ldots s_n\rangle$, $s_i \in \Gamma_i$, $i = 1, \ldots, n$. Cada um dos estados base $|s_1 s_2 \ldots s_n\rangle$ identifica-se naturalmente com o produto tensorial dos correspondentes estados base dos subsistemas: $|s_1\rangle \otimes |s_2\rangle \otimes \ldots \otimes |s_n\rangle$. Daqui decorre a equivalência entre os conceitos de Γ–qudit composto e sistema quântico composto referido no Postulado 2.

Teorema 2.1. Dadas as linguagens Γ_i, $i \in [1 \,..\, n]$, e a correspondente linguagem produto $\Gamma = \prod_{i=1}^{n} \Gamma_i$, então

$$\mathcal{H}(\Gamma) \cong \bigotimes_{i=1}^{n} \mathcal{H}(\Gamma_i) \quad .$$

Demonstração. Para $s \in \Gamma$, $\exists^1 s_1 \in \Gamma_1, \exists^1 s_2 \in \Gamma_2, \ldots, \exists^1 s_n \in \Gamma_n$ tais que $s = s_1 s_2 \ldots s_n$.

Seja $\mathbf{U}\,|s\rangle = |s_1\rangle \otimes |s_2\rangle \otimes \ldots \otimes |s_n\rangle$, $s \in \Gamma$. $\mathbf{U}$ é claramente uma correspondência biunívoca entre a base computacional de $\mathcal{H}(\Gamma)$ e uma base ortonormada de $\bigotimes_{i=1}^{n} \mathcal{H}(\Gamma_i)$, pelo que a extensão linear de $\mathbf{U}$ ao espaço $\mathcal{H}(\Gamma)$ constitui um isomorfismo de espaços de Hilbert. □

Definição 2.5. Considere-se uma linguagem produto Γ da forma $\Gamma = \Gamma_1\Gamma_2$. Diz-se que o estado $|\psi\rangle \in \mathcal{H}(\Gamma)$ é um *estado produto*, relativamente a uma factorização $\mathcal{H}(\Gamma) = \mathcal{H}(\Gamma_1) \otimes \mathcal{H}(\Gamma_2)$, se existem $|\psi_1\rangle \in \mathcal{H}(\Gamma_1)$ e $|\psi_2\rangle \in \mathcal{H}(\Gamma_2)$ tais que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Caso contrário, $|\psi\rangle$ diz-se um *estado entrelaçado*.

Cada Γ–qudit composto, ψ, é constituído por $n = \mathrm{comp}(\Gamma)$ qudits $\psi_1, \psi_2, \ldots, \psi_n$, cada ψ_i um Γ_i–qudit. Em geral, para indexar os qudits de um Γ–qudit composto recorre-se a um *conjunto de índices*[1], possivelmente distinto do conjunto $[1 \,..\, n]$ na enumeração anterior. Desta forma, qualquer sistema quântico composto é visto como um registo cujos elementos são qudits.

Definição 2.6. Um Γ–*registo quântico* é um par (ψ, I) em que ψ é um Γ–qudit e I um conjunto de índices de cardinal $|I| = \mathrm{comp}(\Gamma)$.

Considere-se na definição anterior o conjunto de índices $I = [i_1 \,..\, i_n]$. Então $\Gamma = \prod_{j=1}^{n} \Gamma_{i_j}$ e para cada $j \in [1 \,..\, n]$, ψ_{i_j} é um Γ_{i_j}–qudit, o qudit de ordem j do registo.

Definição 2.7. Para $J \subseteq I$, o par (ϕ, J) é um *subregisto* de (ψ, I) sempre que $\forall j \in J$, $\phi_j = \psi_j$.

Considere-se um conjunto de índices I e uma linguagem produto $\Gamma = \prod_{i \in I} \Gamma_i$. Para $J \subseteq I$, a linguagem $\prod_{j \in J} \Gamma_j$ denota-se simplesmente por Γ_J. Assim $\Gamma = \Gamma_I$ e na definição anterior ϕ é um Γ_J–qudit e (ϕ, J) um Γ_J–registo quântico.

[1] Um conjunto de índices é formalmente o domínio I de uma função sobrejectiva $f : I \to X$. Para cada $i \in I$, em vez de $f(i)$ escreve-se f_i. Assim $X = \{f_i : i \in I\}$. Uma ordem no conjunto de índices induz naturalmente uma ordem no conjunto indexado, i.e, para $i, j \in I$ se $i < j$ então $f_i < f_j$.

2.2 Portas quânticas

Após a especificação do conceito de estado de um sistema quântico importa agora analisar a sua dinâmica. Nesta tese consideram-se apenas sistemas quânticos fechados pelo que não é necessário recorrer ao formalismo dos operadores de densidade e superoperadores para descrever a sua evolução.

> **Postulado 3:** *A evolução de um sistema quântico fechado é descrita por uma transformação unitária definida no espaço de estados do sistema. Isto é, o estado* $|\psi\rangle$ *num instante* t_1 *relaciona-se com o estado* $|\phi\rangle$ *num instante posterior* t_2 *por intermédio de um operador unitário* $\mathbf{U}$ *que depende apenas dos instantes* t_1 *e* t_2*:*
>
> $$|\phi\rangle = \mathbf{U}\,|\psi\rangle \quad .$$

Um exemplo trivial da descrição da evolução de um sistema quântico por intermédio de operadores unitários é dado pelo *operador identidade*. Este operador unitário definido sobre o espaço de Hilbert $\mathcal{H}(\Gamma)$ subjacente a um Γ–qudit denota-se por $\mathbf{I}_\Gamma$. A acção $|\psi\rangle = \mathbf{I}_\Gamma\,|\psi\rangle$ indica que, como resultado da evolução entre dois instantes específicos, o estado final do sistema quântico é idêntico ao seu estado inicial.

Considere-se um conjunto de índices $I = [i_1 \,..\, i_n]$ e uma permutação $\boldsymbol{\pi}$ de $[1 \,..\, n]$. Denota-se por $\boldsymbol{\pi}(I)$ o conjunto de índices $\left[i_{\boldsymbol{\pi}(1)} \,..\, i_{\boldsymbol{\pi}(n)}\right]$. O símbolo $\boldsymbol{\pi}$ é ainda utilizado para identificar a função bijectiva $i_j \mapsto i_{\boldsymbol{\pi}(j)}$, $j \in [1 \,..\, n]$, dizendo-se que $\boldsymbol{\pi}$ é uma permutação de I.

Assim, se Γ_I é uma linguagem produto de comprimento n então $\Gamma_{\boldsymbol{\pi}(I)}$ denota a linguagem $\Gamma_{i_{\boldsymbol{\pi}(1)}}\Gamma_{i_{\boldsymbol{\pi}(2)}}\cdots\Gamma_{i_{\boldsymbol{\pi}(n)}}$. Em particular, quando Γ é uma linguagem produto de n linguagens e $\boldsymbol{\pi}$ é uma permutação de $[1 \,..\, n]$, denota-se a linguagem $\Gamma_{\boldsymbol{\pi}([1 \,..\, n])}$ simplesmente por $\Gamma_{\boldsymbol{\pi}}$.

Qualquer permutação $\boldsymbol{\pi}$ de I induz um isomorfismo entre as linguagens Γ_I e $\Gamma_{\boldsymbol{\pi}(I)}$, representado ainda pelo mesmo símbolo $\boldsymbol{\pi} : \Gamma_I \to \Gamma_{\boldsymbol{\pi}(I)}$ e definido por

$$\boldsymbol{\pi}(s_{i_1}s_{i_2}\cdots s_{i_n}) = s_{i_{\boldsymbol{\pi}(1)}}s_{i_{\boldsymbol{\pi}(2)}}\cdots s_{i_{\boldsymbol{\pi}(n)}},\ s_{i_j} \in \Gamma_{i_j},\ j \in [1 \,..\, n] \quad .$$

Este isomorfismo entre linguagens admite uma extensão natural a um isomorfismo entre os espaços de Hilbert associados às linguagens, na forma de um *operador de permutação lógica*[2], um operador linear $\mathbf{P}_{\boldsymbol{\pi}} : \mathcal{H}(\Gamma_I) \to \mathcal{H}(\Gamma_{\boldsymbol{\pi}(I)})$ definido por

$$\mathbf{P}_{\boldsymbol{\pi}} |s\rangle = |\boldsymbol{\pi}(s)\rangle \, , s \in \Gamma_I .$$

Definição 2.8. Considerem-se uma linguagem produto Γ_I, um conjunto de índices $J \subseteq I$ e um operador linear $\mathbf{A}$ em $\mathcal{H}(\Gamma_J)$. A *extensão* linear de $\mathbf{A}$ a $\mathcal{H}(\Gamma_I)$ é o operador linear $\mathbf{A}[J] : \mathcal{H}(\Gamma_I) \to \mathcal{H}(\Gamma_I)$ definido por

$$\mathbf{A}[J] = \mathbf{P}_{\boldsymbol{\pi}}^{\dagger} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K}) \cdot \mathbf{P}_{\boldsymbol{\pi}} \quad ,$$

onde $K = I \setminus J$ e $\boldsymbol{\pi}$ é a permutação de I tal que $\boldsymbol{\pi}(I) = JK$.

Observação 2.2. No seguinte sentido, a extensão de um operador é independente da permutação lógica considerada: se, no lugar da permutação $\boldsymbol{\pi}$ na definição anterior, se considerar uma qualquer permutação $\bar{\boldsymbol{\pi}}$ de I tal que $\bar{\boldsymbol{\pi}}(I) = JL$ (com $I = J \cup L$) então $\mathbf{P}_{\boldsymbol{\pi}}^{\dagger} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K}) \cdot \mathbf{P}_{\boldsymbol{\pi}} = \mathbf{P}_{\bar{\boldsymbol{\pi}}}^{\dagger} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\bar{\boldsymbol{\pi}}}$.

A definição anterior permite traduzir a noção de acção local de um operador unitário. Em primeiro lugar observe-se que qualquer extensão de um operador unitário $\mathbf{U}$ é ainda um operador unitário e, a menos de uma permutação de índices, $\mathbf{U}[J]$ é idêntico a $\mathbf{U} \otimes \mathbf{I}_{\Gamma_K}$.

Suponha-se que o estado inicial de um sistema quântico é, a menos de uma permutação de índices, um estado produto $|\psi\rangle \otimes |\phi\rangle$ com $|\psi\rangle \in \mathcal{H}(\Gamma_J)$ e $|\phi\rangle \in \mathcal{H}(\Gamma_K)$. Então como resultado da acção do operador $\mathbf{U}[J]$ obtém-se, a menos de um permutação de índices, o estado $(\mathbf{U}|\psi\rangle) \otimes |\phi\rangle$ pelo que o estado dos qudits do sistema indexados por K é invariante relativamente à acção de $\mathbf{U}[J]$.

Num sentido similar, o operador $\mathbf{U}[J]$ também não afecta os qudits indexados por K quando o estado do sistema é entrelaçado, embora não seja agora possível afirmar que o estado

[2]Uma permutação lógica de qudits é essencialmente uma ferramenta matemática que permite reordenar os qudits de um sistema consoante seja conveniente de modo a simplificar o enunciado de definições e a demonstração de resultados. Em claro contraste com o conceito de permutação de informação, não se atribui significado físico às permutações lógicas, pelo menos a um nível quântico.

dos qudits indexados por K é invariante relativamente à acção de $\mathbf{U}[J]$. (O entrelaçamento não permite sequer considerar a noção do estado dos qudits indexados por K!) Mais precisamente, a menos de uma permutação de índices, é sempre possível escrever o estado do sistema na forma $\sum_k |\psi_k\rangle \otimes |\phi_k\rangle$, com $|\psi_k\rangle \in \mathcal{H}(\Gamma_J)$ e $|\phi_k\rangle \in \mathcal{H}(\Gamma_K)$. Como simples consequência da linearidade, o resultado da acção do operador $\mathbf{U}[J]$ sobre o sistema quântico é, a menos de uma permutação de índices, $\sum_k (\mathbf{U}\,|\psi_k\rangle) \otimes |\phi_k\rangle$.

De uma forma simplista, uma computação quântica consiste na preparação inicial de um sistema quântico e no controlo da evolução do estado do sistema pela utilização, em série e ou em paralelo, de controlos locais. Cada controlo é modelado pela acção $\mathbf{U}[J]$ de um operador unitário $\mathbf{U}$ sobre um pequeno número de qudits do sistema. O estudo de processos que permitem a realização física de tais controlos, i.e, a implementação da acção local de operadores unitários, constitui uma importante área da Computação Quântica repleta de árduos problemas de natureza prática, aqui não tratados. Com a seguinte definição obtém-se a abstracção necessária para prosseguir o desenvolvimento do modelo ao nível teórico[3].

Definição 2.9. Para uma linguagem Γ, uma Γ*–porta quântica* é uma realização de um operador unitário em $\mathcal{H}(\Gamma)$.

Conclui-se esta secção com a demonstração de dois resultados muito úteis relacionados com o produto das extensões de operadores com acção em conjuntos disjuntos de qudits de um sistema: a relação do produto das extensões com o produto tensorial dos operadores e a comutatividade das extensões. Para uma linguagem Γ, denota-se por $\mathcal{U}(\Gamma)$ o conjunto dos operadores unitários em $\mathcal{H}(\Gamma)$.

Lema 2.1. Considerem-se uma linguagem produto Γ_I, conjuntos de índices $J, K \subset I$ e os operadores $\mathbf{A} \in \mathcal{U}(\Gamma_J)$, $\mathbf{B} \in \mathcal{U}(\Gamma_K)$. Se $J \cap K = \emptyset$ então $\mathbf{A}[J] \cdot \mathbf{B}[K] = (\mathbf{A} \otimes \mathbf{B})\,[JK]$.

Demonstração. Tendo em conta a observação 2.2 sobre a independência das extensões de operadores relativamente a permutações lógicas, sejam $\mathbf{A}[J] = \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}}$

[3]Por vezes misturam-se os conceitos de porta quântica e operador unitário. De certa forma os conceitos são equivalentes: a funcionalidade de uma porta quântica traduz-se por um operador unitário e cada operador unitário é (pelo menos teoricamente) realizável por uma porta ou circuito quântico.

e $\mathbf{B}[K] = \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{B}} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}}$, onde $\boldsymbol{\pi}_\mathbf{A}$ e $\boldsymbol{\pi}_\mathbf{B}$ são permutações de I tais que $\boldsymbol{\pi}_\mathbf{A}(I) = J(KL)$ e $\boldsymbol{\pi}_\mathbf{B}(I) = K(JL)$ para $L = I \setminus JK$.

Por inserção de $\mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} = \mathbf{I}_{\Gamma_I}$ à direita do produto $\mathbf{A}[J] \cdot \mathbf{B}[K]$ obtém-se

$$\begin{aligned}\mathbf{A}[J] \cdot \mathbf{B}[K] &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{B}} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \\ &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \\ &\qquad \Big((\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}})^{\dagger} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot (\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}}) \Big) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \quad .\end{aligned} \tag{2.3}$$

Uma vez que $\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}}$ constitui uma permutação lógica de $\mathcal{H}(\Gamma_J\Gamma_K\Gamma_L)$ em $\mathcal{H}(\Gamma_K\Gamma_J\Gamma_L)$ então $(\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}})^{\dagger} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot (\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}}) = \mathbf{I}_{\Gamma_J} \otimes \mathbf{B} \otimes \mathbf{I}_{\Gamma_L}$. Assim,

$$\begin{aligned}\mathbf{A}[J] \cdot \mathbf{B}[K] &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot (\mathbf{I}_{\Gamma_J} \otimes \mathbf{B} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \\ &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{B} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \\ &= (\mathbf{A} \otimes \mathbf{B})[JK] \quad .\end{aligned} \tag{2.4}$$

A igualdade verifica-se pelo simples facto de $\boldsymbol{\pi}_\mathbf{A}$ constituir uma permutação de I tal que $\boldsymbol{\pi}_\mathbf{A}(I) = (JK)L$. □

Lema 2.2. Considerem-se uma linguagem produto Γ_I, conjuntos de índices $J, K \subset I$ e os operadores $\mathbf{A} \in \mathcal{U}(\Gamma_J)$, $\mathbf{B} \in \mathcal{U}(\Gamma_K)$. Se $J \cap K = \emptyset$ então os operadores $\mathbf{A}[J]$ e $\mathbf{B}[K]$ comutam, i.e, $\mathbf{A}[J] \cdot \mathbf{B}[K] = \mathbf{B}[K] \cdot \mathbf{A}[J]$.

Demonstração. Considerem-se as permutações $\boldsymbol{\pi}_\mathbf{A}$ e $\boldsymbol{\pi}_\mathbf{B}$ definidas na demonstração do lema anterior.

Por inserção de $\mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} = \mathbf{I}_{\Gamma_I}$ à esquerda do produto $\mathbf{B}[K] \cdot \mathbf{A}[J]$ obtém-se

$$\begin{aligned}\mathbf{B}[K] \cdot \mathbf{A}[J] &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{B}} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \\ &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot \Big((\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}})^{\dagger} \cdot (\mathbf{B} \otimes \mathbf{I}_{\Gamma_J} \otimes \mathbf{I}_{\Gamma_L}) \cdot (\mathbf{P}_{\boldsymbol{\pi}_\mathbf{B}} \cdot \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}}) \Big) \cdot \\ &\qquad (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \\ &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{I}_{\Gamma_J} \otimes \mathbf{B} \otimes \mathbf{I}_{\Gamma_L}) \cdot (\mathbf{A} \otimes \mathbf{I}_{\Gamma_K} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}} \\ &= \mathbf{P}^{\dagger}_{\boldsymbol{\pi}_\mathbf{A}} \cdot (\mathbf{A} \otimes \mathbf{B} \otimes \mathbf{I}_{\Gamma_L}) \cdot \mathbf{P}_{\boldsymbol{\pi}_\mathbf{A}}\end{aligned} \tag{2.5}$$

Comparando esta última igualdade com (2.3) imediatamente se conclui que $\mathbf{B}[K] \cdot \mathbf{A}[J] = \mathbf{A}[J] \cdot \mathbf{B}[K]$. □

2.2.1 Portas quânticas elementares e universalidade

É sabido, no contexto da Computação Clássica, que um conjunto finito de portas lógicas, e.g $\{\text{AND}, \text{OR}, \text{NOT}\}$, é suficiente para realizar qualquer função booleana na forma de um circuito.

No modelo de Computação Quântica em sistemas de qubits conhecem-se resultados análogos. Por exemplo, as portas quânticas correspondentes aos operadores unitários num qubit mais a porta de dois qubits **CNOT** formam um conjunto universal na medida em que qualquer operador unitário é realizável de forma exacta por um circuito quântico baseado nessas portas.

Note-se que um conjunto finito de portas quânticas jamais poderá ser exactamente universal já que o conjunto dos operadores unitários num espaço de Hilbert é contínuo, enquanto o conjunto de circuitos baseados num conjunto finito de portas quânticas é apenas enumerável. Em Brylinski e Brylinski [9] encontra-se uma caracterização dos conjuntos de portas quânticas (exactamente) universais em computação com sistemas de qudits (não híbridos). Por outro lado cada operador unitário é realizável de forma aproximada, e com qualquer grau de precisão, recorrendo apenas a um conjunto finito de portas quânticas.

A questão da universalidade é ainda um problema pouco estudado em Computação Quântica em Sistemas Híbridos. Recentemente, no trabalho de Khan e Perkowski [32] surge uma notável excepção. Partindo de uma generalização do método de decomposição matricial coseno–seno, aqueles autores mostram ser possível escrever qualquer operador unitário no espaço de Hilbert subjacente a um qualquer sistema híbrido de qudits na forma de um produto de operadores elementares, interpretado como um circuito quântico constituído por multiplexadores, implementados com portas de controlo do tipo Muthukrishnan-Stroud [37] e portas de rotação de Givens.

A importância destes resultados situa-se primariamente ao nível teórico já que em geral a decomposição de um operador unitário num sistema (híbrido) de n qudits é realizada à custa de um número exponencial (em n) de portas quânticas elementares.

Continua em aberto o problema da síntese óptima de circuitos quânticos para um dado operador unitário num sistema (híbrido) de qudits, embora para o caso de sistemas de qubits

se encontrem várias referências [10], [38].

Seguem-se vários exemplos de portas quânticas para sistemas de Γ–qudits. Porém, antes disso, note-se que é possível definir operações aritméticas numa qualquer linguagem Γ de tamanho $d = |\Gamma|$ como extensões naturais das operações aritméticas modulares em $\mathbb{Z}_d$. Por exemplo, fala-se da adição e subtracção modulares de palavras (símbolos) de Γ.

Mais precisamente, para cada linguagem considera-se à priori uma enumeração standard das suas palavras, $\natural : \mathbb{Z}_d \to \Gamma$, definindo-se a partir desta as operações aritméticas com palavras. Como exemplos, para $s, t \in \Gamma$ a expressão $(s + t) \bmod \Gamma$ representa a palavra $\natural\left((\natural^{-1}(s) + \natural^{-1}(t)) \bmod d\right)$ e $(s - t) \bmod \Gamma$ a palavra $\natural\left((\natural^{-1}(s) - \natural^{-1}(t)) \bmod d\right)$.

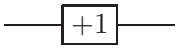
- A porta Identidade

$$\mathbf{I} : \mathcal{H}(\Gamma) \to \mathcal{H}(\Gamma)$$
$$\mathbf{I}\,|s\rangle = |s\rangle\,, s \in \Gamma$$

é apenas uma porta lógica no sentido em que é utilizada como auxiliar na definição de extensões de outras portas, não sendo por isso representada nos circuitos.

- A porta Incremento

$$\mathbf{INC} : \mathcal{H}(\Gamma) \to \mathcal{H}(\Gamma)$$
$$\mathbf{INC}\,|s\rangle = |(s+1) \bmod \Gamma\rangle\,, s \in \Gamma$$



pode ser vista como uma generalização da porta **NOT** em sistemas de qubits. A sua forma matricial é

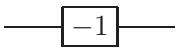
$$\mathbf{INC} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

A aplicação sequencial de $k \in \mathbb{N}$ portas **INC** corresponde à transformação $|s\rangle \mapsto |(s+k) \mod \Gamma\rangle$ como se ilustra na figura 2.1.(Note-se que a expressão $(s+k) \mod \Gamma$ corresponde a uma forma abreviada de escrever $\natural\left((\natural^{-1}(s) + k) \bmod d\right)$ para $d = |\Gamma|$.)

Figura 2.1: Aplicação sequencial de k portas **INC**

- A porta Decremento

  $$\mathbf{DEC} : \mathcal{H}(\Gamma) \to \mathcal{H}(\Gamma)$$
  $$\mathbf{DEC}\,|s\rangle = |(s-1) \bmod \Gamma\rangle\,, s \in \Gamma \in \Gamma$$

  pode também ser vista como uma generalização da porta **NOT** em sistemas de qubits, possui a seguinte representação matricial

  $$\mathbf{DEC} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

  A aplicação sequencial de $k \in \mathbb{N}$ portas **DEC** corresponde à transformação $|s\rangle \mapsto |(s-k) \bmod \Gamma\rangle$ ilustrada na figura 2.2.

Figura 2.2: Aplicação sequencial de k portas **DEC**

- A porta de fase

  $$\mathbf{Z}\,|s\rangle = \omega^s\,|s\rangle$$

  onde ω é uma raiz índice d da unidade (e.g. $\omega = e^{2\pi i/d}$). Note-se que para um qubit, $\mathbf{Z}\,|0\rangle = |0\rangle$ e $\mathbf{Z}\,|1\rangle = -\,|1\rangle$.

- A porta de Rotação de Givens

$$\mathbf{G}^{s,t}(\theta) = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & \cos\theta & \cdots & \sin\theta & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & -\sin\theta & \cdots & \cos\theta & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{bmatrix}$$

onde os valores $\cos\theta$ e $\sin\theta$ ocorrem nas intersecções das linhas e colunas $\natural^{-1}(s)+1$ e $\natural^{-1}(t)+1$.

- Para $t \in \Gamma_1$ e um qualquer operador unitário $\mathbf{U}$ em $\mathcal{H}(\Gamma_2)$ define-se a porta de controlo

$$\mathbf{\Lambda}^t(\mathbf{U}) : \mathcal{H}(\Gamma_1) \otimes \mathcal{H}(\Gamma_2) \to \mathcal{H}(\Gamma_1) \otimes \mathcal{H}(\Gamma_2)$$

$$\mathbf{\Lambda}^t(\mathbf{U})\,|s\rangle \otimes |x\rangle = \begin{cases} |t\rangle \otimes (\mathbf{U}\,|x\rangle) & \text{se } s = t \\ |s\rangle \otimes |x\rangle & \text{caso contrário.} \end{cases}$$

Quando os qudits de controlo se encontram num estado base, a acção desta porta quântica, ilustrada na figura 2.3, consiste em aplicar $\mathbf{U}$ aos qudits alvo se e só se o estado dos qudits de controlo for $|t\rangle$.

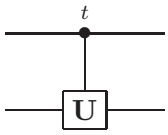


Figura 2.3: Porta genérica de controlo

- Seja $\Gamma = \{s_0, s_1, \ldots, s_{d-1}\}$. Como se ilustra na figura 2.4, o resultado da aplicação sequencial das portas quânticas $\mathbf{\Lambda}^{s_1}(\mathbf{INC})$, $\mathbf{\Lambda}^{s_2}(\mathbf{INC}^2)$, ..., $\mathbf{\Lambda}^{s_{d-1}}(\mathbf{INC}^{d-1})$ a um Γ^2–qudit corresponde ao operador

$$\mathbf{PLUS} : \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma) \to \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma)$$

$$\mathbf{PLUS}\,|s\rangle \otimes |t\rangle = |s\rangle\,|(s+t) \mod \Gamma\rangle\ .$$

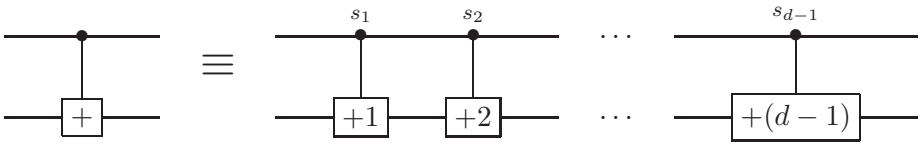


Figura 2.4: A porta quântica **PLUS**

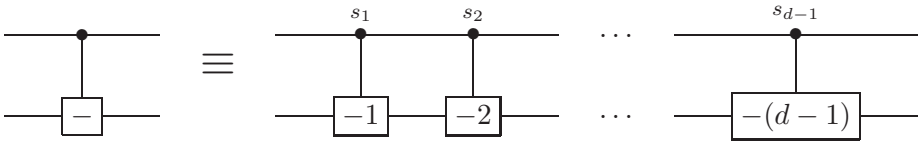


Figura 2.5: A porta quântica **MINUS**

De forma análoga, define-se operador

$$\mathbf{MINUS} : \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma) \to \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma)$$

$$\mathbf{MINUS}\,|s\rangle \otimes |t\rangle = |s\rangle\,|(s-t) \mod \Gamma\rangle\ .$$

A figura 2.5 ilustra uma possível implementação sequencial deste operador.

Quando as dimensões dos espaços de Hilbert são diferentes é ainda possível definir operadores de soma e subtracção parciais. Uma análise de medidas de entrelaçamento relativas a estes operadores encontra-se em Daboul et al. [13].

- É possível utilizar o operador **PLUS** para realizar a cópia do estado de um qudit. Pelo teorema da não clonagem, a operação de cópia exacta do estado de um qudit não é em geral possível. No entanto, a cópia de informação clássica, i.e., dos estados base de um qudit, é sempre possível. Na figura 2.6 ilustra-se a acção do operador de cópia.

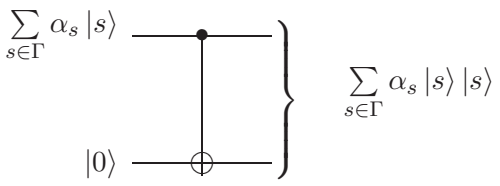


Figura 2.6: A porta quântica de cópia.

2.3 Medição em sistemas quânticos

"*... system, apparatus, environment, microscopic, macroscopic, reversible, irreversible, observable, information, measurement. On this list of bad words the worst of all is measurement.* "

John S. Bell

Desde o início da sua formulação, que se assistiu a uma grande controvérsia em torno do problema da medição em Mecânica Quântica. A polémica eternizada com a celebre frase de Einstein "*Deus não joga aos dados*" originou acesos debates, muitas vezes com cariz metafísico. Actualmente persiste ainda alguma sensação de desconforto em torno da origem da probabilidade na teoria quântica.

Como se referiu no capítulo 1, a medição de um sistema quântico segundo um observável reduz o estado do sistema a um vector próprio do subespaço próprio do valor próprio observado. Mais precisamente, considere-se a decomposição espectral de um observável num espaço de Hilbert $\mathcal{H}$, $\mathbf{A} = \sum_m m\mathbf{P}_m$ e $|\psi\rangle$ o estado de um sistema quântico em $\mathcal{H}$. A probabilidade de observar o valor m na medição de $|\psi\rangle$ é $\text{prob}(m) = \langle\psi|\,\mathbf{P}_m\,|\psi\rangle$ e se m é o resultado da medição do estado $|\psi\rangle$ então o estado após a medição é dado por $\frac{\mathbf{P}_m|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_m|\psi\rangle}}$. Existem outras formulações do conceito de medição de um sistema quântico. Por exemplo em Kitaev et al. [33] é possível encontrar o seguinte:

> **Postulado 4:** *Uma medição quântica é descrita por uma colecção* $\{\mathbf{M}_m\}$ *de operadores lineares definidos no espaço de estados do sistema quântico a ser medido, que satisfaça a relação de completude* $\sum_m \mathbf{M}_m^\dagger\mathbf{M}_m = \mathbf{I}$. *O índice* m *indica o possível resultado da medição. Se* $|\psi\rangle$ *é o estado de um sistema quântico antes da observação então a probabilidade de se observar o resultado* m *é dada por* $\text{prob}(m) = \langle\psi|\,\mathbf{M}_m^\dagger\mathbf{M}_m\,|\psi\rangle$. *O estado do sistema após a observação do valor* m *é*
>
> $$\frac{\mathbf{M}_m\,|\psi\rangle}{\sqrt{\langle\psi|\,\mathbf{M}_m^\dagger\mathbf{M}_m\,|\psi\rangle}} \quad .$$

Não é difícil verificar que as medições espectrais de Von Neumman segundo projecções ortogonais constituem um caso particular do postulado 4. Para além disso, prova-se que

qualquer medição segundo este postulado é realizável por medições espectrais projectivas ortogonais num sistema quântico estendido, por introdução de sistemas auxiliares, desde que precedidas pela acção de um conjunto adequado de operadores unitários.

Nesta tese consideram-se apenas medições na base computacional, generalizações da regra de Born (em homenagem ao físico Max Born por estabelecer a relação entre o caracter probabilístico dos resultados das medições e as amplitudes das sobreposição de estados base).

Definição 2.10. A *medição na base computacional* de um Γ–qudit é a medição pelo conjunto completo de projectores ortogonais $\{|s\rangle\langle s| : s \in \Gamma\}$.

Teorema 2.2 (Medição de um Γ–qudit na base computacional)**.** Seja $|\psi\rangle = \sum_{s\in\Gamma} \alpha_s |s\rangle$ o estado de um Γ–qudit. A probabilidade de observar $s \in \Gamma$ por medição na base computacional de $\mathcal{H}(\Gamma)$ é

$$\text{prob}(s) = |\alpha_s|^2 . \tag{2.6}$$

Se s é o valor observado então o estado pós-medição é, a menos de uma fase global, idêntico a $|s\rangle$.

Demonstração. Considerem-se os operadores $\mathbf{M}_s = |s\rangle\langle s|$, $s \in \Gamma$. Para cada $s \in \Gamma$, $\mathbf{M}_s$ é um projector, i.e, $\mathbf{M}_s^2 = \mathbf{M}_s$ e $\mathbf{M}_s^\dagger = \mathbf{M}_s$ pelo que $\mathbf{M}_s^\dagger \mathbf{M}_s = \mathbf{M}_s$. Verifica-se facilmente que $\sum_{s\in\Gamma} \mathbf{M}_s = \mathbf{I}_\Gamma$.

Assim o conjunto $\{\mathbf{M}_s : s \in \Gamma\}$ satisfaz a relação de completude e a a probabilidade de observar s é, pelo postulado 4, $\text{prob}(s) = \langle\psi| \mathbf{M}_m^\dagger \mathbf{M}_m |\psi\rangle = \langle\psi| \mathbf{M}_m |\psi\rangle = \langle\psi| |s\rangle\langle s| |\psi\rangle = \langle\psi|s\rangle \langle s|\psi\rangle = \alpha_s^* \alpha_s = |\alpha_s|^2$. Finalmente, o estado pós-medição é $\frac{\mathbf{M}_s^\dagger \mathbf{M}_s |\psi\rangle}{\sqrt{\langle\psi|\mathbf{M}_s^\dagger \mathbf{M}_s|\psi\rangle}} = \frac{\alpha_s}{|\alpha_s|} |s\rangle$. A fase global $e^{i\theta} = \frac{\alpha_s}{|\alpha_s|}$ pode ser ignorada uma vez que não possível distinguir os estados $|s\rangle$ e $e^{i\theta} |s\rangle$ com qualquer medição quântica [33]. □

Se $R = (\psi, I)$ é um Γ–registo quântico então medir o registo R na base computacional significa medir o estado do Γ–qudit ψ na base computacional, ou seja, medir todos os qudits do registo. E quando se pretende medir apenas alguns dos qudits de um registo quântico?

Definição 2.11. A *medição na base computacional de um subregisto* $S = (\phi, J)$ de um Γ–registo quântico $R = (\psi, I)$ é a medição com o conjunto completo de projectores ortogonais $\{|t\rangle\langle t|\,[J] : t \in \Gamma_J\}$.

Na definição anterior $|t\rangle\langle t|\,[J]$ denota a extensão a $\mathcal{H}(\Gamma)$ do projector $|t\rangle\langle t|$ em $\mathcal{H}(\Gamma_J)$. No resultado seguinte explicitam-se a distribuição de probabilidade e a transição de estado associados a uma medição de um subregisto.

Teorema 2.3. Sejam $S = (\phi, J)$ um subregisto de um Γ–registo quântico $R = (\psi, I)$, $K = I \setminus J$ e $\boldsymbol{\pi}$ a permutação de I tal que $\boldsymbol{\pi}(I) = JK$. Se o estado do registo R é $|\psi\rangle = \sum_{s\in\Gamma} \alpha_s |s\rangle$ então a probabilidade de observar $t \in \Gamma_J$ por medição na base computacional do subregisto S de R é

$$\text{prob}(t) = \sum_{u\in\Gamma_K} \left|\alpha_{\boldsymbol{\pi}^{-1}(tu)}\right|^2 \tag{2.7}$$

e se t for o valor observado então o estado pós-medição do registo R é

$$\sum_{u\in\Gamma_K} \frac{\alpha_{\boldsymbol{\pi}^{-1}(tu)}}{\sqrt{\text{prob}(t)}} \left|\boldsymbol{\pi}^{-1}(tu)\right\rangle \quad . \tag{2.8}$$

Demonstração. Verifica-se facilmente que os operadores $\mathbf{M}_t = |t\rangle\langle t|\,[J]$, $t \in \Gamma_J$, são projectores dois a dois ortogonais e satisfazem a relação de completude $\sum_{t\in\Gamma_J} \mathbf{M}_t = \mathbf{I}_\Gamma$.

Assim, pelo postulado 4, a probabilidade de observar $t \in \Gamma_J$ é

$$\begin{aligned}\text{prob}(t) &= \langle\psi|\,\mathbf{M}_t^\dagger \mathbf{M}_t\,|\psi\rangle = \langle\psi|\,(\mathbf{P}_{\boldsymbol{\pi}}^\dagger \cdot |t\rangle\langle t| \otimes \mathbf{I}_{\Gamma_K} \cdot \mathbf{P}_{\boldsymbol{\pi}})\,|\psi\rangle \\ &= (\mathbf{P}_{\boldsymbol{\pi}}\,|\psi\rangle)^\dagger \cdot |t\rangle\langle t| \otimes \mathbf{I}_{\Gamma_K} \cdot (\mathbf{P}_{\boldsymbol{\pi}}\,|\psi\rangle) \quad .\end{aligned}$$

Uma vez que $\boldsymbol{\pi}$ define uma correspondência biunívoca entre $\Gamma = \Gamma_I$ e $\Gamma_J\Gamma_K$, é possível reescrever o estado do registo R, $|\psi\rangle = \sum_{s\in\Gamma} \alpha_s |s\rangle$, na seguinte forma:

$$|\psi\rangle = \sum_{w\in\Gamma_J} \sum_{u\in\Gamma_K} \alpha_{\boldsymbol{\pi}^{-1}(wu)} \left|\boldsymbol{\pi}^{-1}(wu)\right\rangle \quad .$$

Segue-se que $\mathbf{P}_{\boldsymbol{\pi}}\,|\psi\rangle = \sum_{w\in\Gamma_J} \sum_{u\in\Gamma_K} \alpha_{\boldsymbol{\pi}^{-1}(wu)} |wu\rangle$ e portanto

$$(|t\rangle\langle t| \otimes \mathbf{I}_{\Gamma_K}) \cdot \mathbf{P}_{\boldsymbol{\pi}}\,|\psi\rangle = \sum_{u\in\Gamma_K} \alpha_{\boldsymbol{\pi}^{-1}(tu)} |tu\rangle \quad .$$

Observando que $(\mathbf{P}_{\boldsymbol{\pi}} |\psi\rangle)^\dagger = \sum_{w\in\Gamma_J} \sum_{u\in\Gamma_K} \alpha^*_{\boldsymbol{\pi}^{-1}(wu)} \langle wu|$ conclui-se que

$$\begin{aligned}\text{prob}(t) &= (\mathbf{P}_{\boldsymbol{\pi}} |\psi\rangle)^\dagger \cdot |t\rangle\langle t| \otimes \mathbf{I}_{\Gamma_K} \cdot (\mathbf{P}_{\boldsymbol{\pi}} |\psi\rangle) \\ &= \sum_{u\in\Gamma_K} \alpha^*_{\boldsymbol{\pi}^{-1}(tu)} \alpha_{\boldsymbol{\pi}^{-1}(tu)} = \sum_{u\in\Gamma_K} \left|\alpha_{\boldsymbol{\pi}^{-1}(tu)}\right|^2 \quad .\end{aligned}$$

A fórmula (2.8), relativa ao estado pós-medição do registo R, é consequência directa do postulado 4, ao se observar que

$$\begin{aligned}\mathbf{M}_t |\psi\rangle &= \mathbf{P}^\dagger_{\boldsymbol{\pi}} \cdot (|t\rangle\langle t| \otimes \mathbf{I}_{\Gamma_K}) \cdot \mathbf{P}_{\boldsymbol{\pi}} |\psi\rangle = \mathbf{P}^\dagger_{\boldsymbol{\pi}} \Big(\sum_{u\in\Gamma_K} \alpha_{\boldsymbol{\pi}^{-1}(tu)} |tu\rangle \Big) \\ &= \sum_{u\in\Gamma_K} \alpha_{\boldsymbol{\pi}^{-1}(tu)} \left|\boldsymbol{\pi}^{-1}(tu)\right\rangle \quad .\end{aligned}$$

□

2.4 Circuitos quânticos

Informalmente um circuito quântico consiste num conjunto finito de portas e fios quânticos e representa a forma como os fios se ligam às portas. Um circuito quântico pode ainda ser visto como uma descrição de como decompor um operador em portas quânticas.

Definição 2.12. Considere-se uma linguagem produto Γ de comprimento n. Um Γ–*circuito quântico* C é uma sequência de pares $(\mathbf{U}_1, I_1), (\mathbf{U}_2, I_2), \ldots, (\mathbf{U}_m, I_m)$ em que:

- $I_j \subseteq [1 \,..\, n]$ é um conjunto não vazio de índices;
- $\mathbf{U}_j$ é um operador unitário em $\mathcal{U}(\Gamma_{I_j})$.

O *operador unitário* em $\mathcal{U}(\Gamma)$ *realizado pelo circuito* C é

$$\mathbf{U}_C = \mathbf{U}_m[I_m] \cdot \mathbf{U}_{m-1}[I_{m-1}] \cdots \mathbf{U}_2[I_2] \cdot \mathbf{U}_1[I_1].$$

Considere-se um Γ–circuito quântico $C = (\mathbf{U}_1, I_1), (\mathbf{U}_2, I_2), \ldots, (\mathbf{U}_m, I_m)$. O *tamanho* de C é dado pelo número de portas, m, do circuito. Diz-se que C é um Γ–circuito quântico de n qudits se $\text{comp}(\Gamma) = n$. Se $\mathbf{U}$ é uma porta quântica então a expressão $\mathbf{U} \in C$ significa que existe $j \in [1 \,..\, m]$ tal que $\mathbf{U} = \mathbf{U}_j$. Também $(\mathbf{U}, I) \in C$ significa que $\mathbf{U} = \mathbf{U}_j$ e $I = I_j$ para algum $j \in [1 \,..\, m]$.

2.4.1 Grafo de um circuito quântico

Associa-se a cada circuito quântico um grafo dirigido acíclico (uma rede computacional [55]) em que os vértices iniciais e finais correspondem, respectivamente, às entradas e saídas do circuito e cujos vértices interiores são as portas quânticas do circuito.

Este conceito tem sido tratado de uma forma um tanto ou quanto informal, geralmente introduzido por analogia com os grafos de circuitos booleanos no modelo clássico. No entanto as diferenças significativas entre os modelos de circuitos clássicos e quânticos transitam para os respectivos grafos, donde o estudo das propriedades dos grafos de circuitos quânticos constitui um assunto importante *per se*.

Em seguida propõe-se um caracterização formal para o conceito de grafo de um circuito quântico e deduzem-se algumas propriedades fundamentais.

Definição 2.13. Seja $C = (\mathbf{U}_1, I_1), \ldots, (\mathbf{U}_m, I_m)$ um Γ–circuito quântico de n qudits. O grafo associado ao circuito quântico C é o multigrafo dirigido $G(C) = (V, E)$ definido por:

1. Um conjunto de $m + 2n$ vértices particionado em $V = S \cup P \cup T$ onde:

   (a) $S = S(C)$ é um conjunto de n *vértices iniciais*, cada um com semigrau incidente 0 e semigrau emergente 1;

   (b) $T = T(C)$ é um conjunto de n *vértices finais*, cada um com semigrau incidente 1 e semigrau emergente 0;

   (c) $P = P(C)$ é um conjunto de m *vértices interiores*, cada um com semigrau incidente igual ao semigrau emergente.

2. Os vértices iniciais são rotulados por $\ell_S : S \to [1 \,..\, n]$, os vértices finais por $\ell_T : T \to [1 \,..\, n]$ e os vértices interiores por $\ell_P : P \to [1 \,..\, m]$.

3. Seja $\kappa : V \to [1 \,..\, 2n + m]$ a função definida por

$$\kappa(v) = \begin{cases} \ell_S(v) & \text{se } v \in S \\ n + \ell_P(v) & \text{se } v \in P \\ n + m + \ell_T(v) & \text{se } v \in T \end{cases} .$$

Considere-se ainda a função $\Lambda : V \to 2^{[1\,..\,n]}$ definida por

$$\Lambda(v) = \begin{cases} \{\ell_S(v)\} & \text{se } v \in S \\ \{\ell_T(v)\} & \text{se } v \in T \\ I_{\ell_P(v)} & \text{se } v \in P \end{cases} .$$

Existe um e um só arco de $u \in V$ para $v \in V$ rotulado com o inteiro $i \in [1\,..\,n]$ se e só se verificam as três condições:

$$\kappa(u) < \kappa(v); \tag{2.9a}$$

$$i \in \Lambda(u) \cap \Lambda(v); \tag{2.9b}$$

$$\forall j \in [\kappa(u) + 1\,..\,\kappa(v) - 1]\,, i \notin \Lambda(\kappa^{-1}(j)) \quad . \tag{2.9c}$$

Observação 2.3. Na definição anterior a rotulação dos vértices interiores permite associar univocamente cada porta quântica do circuito a um operador unitário $\mathbf{U}_j$ bem como ao conjunto de índices I_j. A função κ define essencialmente uma ordem topológica dos vértices do grafo (os vértices iniciais antes dos interiores e estes seguidos pelos finais) de tal modo todos os arcos definidos pelas condições (2.9) são dirigidos para a frente. Por sua vez, a função Λ permite identificar os fios quânticos (os qudits) que entram e saem de cada uma das portas quânticas.

Uma consequência imediata da observação anterior é que os grafos são acíclicos uma vez que todos os arcos são "dirigidos para a frente". Por outro lado os grafos não são necessariamente conexos, embora não existam vértices isolados. Por exemplo, se um qudit não é afectado por qualquer porta quântica do circuito então existe um arco no grafo de um vértice inicial para um vértice final e nesses vértices não incide qualquer outro arco.

Enunciam-se e demonstram-se em seguida algumas propriedades dos grafos associados a circuitos quânticos.

Teorema 2.4. Seja $G(C)$ o grafo associado a um Γ–circuito quântico C. Existe um caminho em $G(C)$ de $u \in V(C)$ para $v \in V(C)$ com todos os arcos no caminho rotulados com o mesmo número i se e só se $\kappa(u) < \kappa(v)$ e $i \in \Lambda(u) \cap \Lambda(v)$.

Demonstração. Considere-se um caminho em $G(C)$ do vértice u para o vértice v dado por uma sequência de arcos $e_1, \ldots, e_k$.

Para cada $j \in [1 \,..\, k]$ sejam u_j a cauda e e v_j a cabeça do arco e_j. Pela definição 2.13, $\kappa(u_j) < \kappa(v_j)$. Uma vez que $u = u_1$, $v = v_k$ e $v_j = u_{j+1}$ para $j \in [1 \,..\, k-1]$, imediatamente se conclui que $\kappa(u) < \kappa(v)$.

Uma vez que e_1 tem rótulo i então, pela definição 2.13, $i \in \Lambda(u)$. De forma análoga, considerando o arco e_k, conclui-se que $i \in \Lambda(v)$.

Reciprocamente, considere-se o conjunto de vértices

$$Q = \{w \in V(C) : \kappa(u) \leq \kappa(w) \leq \kappa(v) \text{ e } i \in \Lambda(w)\}\,.$$

Por hipótese $\kappa(u) < \kappa(v)$, $i \in \Lambda(u)$ e $i \in \Lambda(v)$. Logo Q é não vazio (contém pelo menos os vértices u e v). Seja R a sequência dos elementos de Q ordenada pela função κ. Claramente o primeiro elemento de R é u e o último é v.

A existência de um arco entre cada par consecutivo de vértices na sequência R rotulado com i é consequência imediata da definição 2.13. Logo a sequência R define um caminho em G(C) de u para v com todos os arcos rotulados com i. □

Corolário 2.1. Seja $G(C)$ o grafo associado a um Γ–circuito quântico C. Existe um caminho em $G(C)$ de $s \in S(C)$ para $t \in T(C)$ com todos os arcos no caminho rotulados com o mesmo número i se e só se $\ell_S(s) = \ell_T(t) = i$.

Demonstração. A ordenação dos vértices de $G(C)$ induzida pela função κ implica que $\kappa(s) < \kappa(t)$ quaisquer que sejam os vértices $s \in S(C)$ e $t \in T(C)$. Para além disso, $\Lambda(s) = \{\ell_S(s)\}$. Logo $i \in \Lambda(s)$ se e só se $\ell_S(s) = i$. De modo análogo, $\Lambda(t) = \{\ell_T(t)\}$ pelo que $i \in \Lambda(t)$ se e só se $\ell_T(t) = i$. O enunciado do corolário é portanto uma consequência directa do teorema. □

Teorema 2.5. Seja $G(C)$ o grafo associado a um Γ–circuito quântico C. Sejam $u, v \in V(C)$ tais que $\kappa(u) < \kappa(v)$ e $i \in \Lambda(u) \cap \Lambda(v)$. Então existe um único caminho de u para v com todos os arcos no caminho rotulados com o mesmo número i.

Demonstração. A existência de um caminho de u para v nas condições enunciadas é assegurada pelo teorema 2.4. Resta provar a sua unicidade. Suponha-se então que existem dois caminhos distintos de u para v, $Q = e_1, \ldots, e_k$ e $Q' = e'_1, \ldots, e'_p$, nas condições do enunciado. Sejam j o índice da primeira divergência entre os caminhos Q e Q', i.e., $e_j \neq e'_j$ e $\forall l < j, e_l = e'_l$. Sejam u_j e v_j (u'_j e v'_j), respectivamente, a cauda e a cabeça de e_j (e'_j). Obviamente, $u_j = u'_j$. Se fosse $v_j = v'_j$ então existiriam dois arcos de u_j para v_j rotulados com o inteiro i, o que é impossível pela definição 2.13. Logo $v_j \neq v'_j$ e portanto $\kappa(v_j) < \kappa(v'_j)$ ou $\kappa(v'_j) < \kappa(v_j)$.

Considere-se que $\kappa(v_j) < \kappa(v'_j)$ (o outro caso trata-se de forma análoga). Então $l = \kappa(v_j)$ satisfaz, $\kappa(u'_j) < l < \kappa(v'_j)$ e $i \in \Lambda(v_j)$. Logo, pela definição 2.13, o arco e'_j não poderia existir. □

Teorema 2.6. O conjunto dos arcos do grafo de um Γ–circuito quântico C de n qudits admite uma partição em n caminhos, cada caminho de um vértice de S para um vértice de T e em que todos os arcos num mesmo caminho possuem o mesmo rótulo i.

Demonstração. Como consequência do lema anterior, para cada $i \in [1 \,..\, n]$ existe um único caminho Q_i de $\ell_S^{-1}(i)$ para $\ell_T^{-1}(i)$ com todos os arcos rotulados pelo inteiro i. Existem portanto n caminhos nas condições do enunciado. Resta mostrar que os n caminhos $Q_1, \ldots, Q_n$ esgotam os arcos de $G(C)$.

Considere-se um qualquer arco $e \in E$ de $G(C)$ e seja i o rótulo de e. Sejam u e v, respectivamente a cauda e a cabeça de e. Se $u \notin S(C)$ então pelo lema 2.4 existe um caminho R_1 de $\ell_S^{-1}(i)$ para u. Se $u \in S(C)$ considere-se $R_1 = \emptyset$ (note que neste caso $u = \ell_S^{-1}(i)$). De forma análoga, se $v \notin T(C)$ então o lema 2.4 garante a existência de um caminho R_2 de v para $\ell_T^{-1}(i)$. Se $v \in T(C)$ então considere-se $R_2 = \emptyset$ (já que neste caso $v = \ell_T^{-1}(i)$). Logo R_1, e, R_2 é um caminho de $\ell_S^{-1}(i)$ para $\ell_T^{-1}(i)$. Pelo lema 2.5, necessariamente $Q_i = R_1, e, R_2$ e portanto $e \in Q_i$. □

Assim, num circuito quântico existem n fios quânticos cada fio associado a um dos caminhos definidos pela partição de arcos no teorema anterior (por sua vez cada caminho está

associado a um dos qudits do sistema quântico subjacente). A operação de divisão (*fanout*) de fios comum no modelo clássico de circuitos booleanos é portanto impossível de realizar no modelo de circuitos quânticos. Este facto é também uma consequência do teorema da não clonagem. Por outro lado, na secção 2.5, define-se a porta quântica de *fanout* a qual permite a cópia (clonagem) de informação clássica num circuito quântico.

Após a definição de grafo de um circuito quântico torna-se agora possível estabelecer formalmente a profundidade de um circuito. Qualquer circuito quântico é organizável em níveis[4] de tal forma que as portas quânticas em cada nível são aplicadas em paralelo. Cada circuito quântico pode ser visto como um calculador de uma certa função clássica. Desta forma, assumindo uma mesma unidade de tempo para a acção de cada porta quântica, o número de níveis num circuito está directamente relacionado com o tempo necessário para calcular o valor daquela função para um dado argumento.

Definição 2.14. Seja $\mathbf{U}_j$ uma porta quântica num Γ–circuito quântico C. A *profundidade* de $\mathbf{U}_j$ no circuito C é o inteiro $\mathrm{prof}(\mathbf{U}_j)$ igual ao comprimento do caminho mais longo em $G(C)$ de um vértice $s \in S(C)$ para $\ell_P^{-1}(j)$.

Definição 2.15. Seja C um Γ–circuito quântico e $k \in \mathbb{N}$. Caso seja não vazio,

$$L_k = \{(\mathbf{U}, I) \in C : \mathrm{prof}(\mathbf{U}) = k\}$$

denomina-se o *nível* k de C. A *profundidade do circuito quântico* C é o inteiro $\mathrm{prof}(C) = \max\{k \in \mathbb{N} : L_k \neq \emptyset\}$.

Definiu-se um nível num circuito como um conjunto de portas quânticas. Como se mostra em seguida, dentro de um mesmo nível a ordem das portas não é importante.

Lema 2.3. Sejam $\mathbf{U}_j$ e $\mathbf{U}_k$ duas quaisquer portas de um Γ–circuito quântico C situadas ao mesmo nível. Então $\Lambda(\ell_P^{-1}(j)) \cap \Lambda(\ell_P^{-1}(k)) = \emptyset$.

Demonstração. Se fosse $\Lambda(\ell_P^{-1}(j)) \cap \Lambda(\ell_P^{-1}(k)) \neq \emptyset$ então o grafo do circuito conteria um arco incidente nos vértices $\ell_P^{-1}(j)$ e $\ell_P^{-1}(k)$ e esses vértices não poderiam estar situados no mesmo nível. □

[4] Na literatura encontra-se frequentemente o sinónimo *camada* (trad. da Língua Inglesa, *layer*).

Do lema anterior conclui-se que se $(\mathbf{U}_j, I_j)$ e $(\mathbf{U}_k, I_k)$ são duas quaisquer portas de um Γ–circuito quântico C situadas ao mesmo nível, i.e, tais que $\text{prof}(\mathbf{U}_j) = \text{prof}(\mathbf{U}_k)$ então $\mathbf{U}_j$ e $\mathbf{U}_k$ agem em conjuntos disjuntos de qudits, i.e, $I_j \cap I_k = \emptyset$. Pelo lema 2.2 as portas comutam, ou seja, $\mathbf{U}_j[I_j] \cdot \mathbf{U}_k[I_k] = \mathbf{U}_k[I_k] \cdot \mathbf{U}_j[I_j]$. Para além disso, pelo lema 2.1, é possível realizar ambos os operadores em paralelo:

$$\mathbf{U}_j[I_j] \cdot \mathbf{U}_k[I_k] = (\mathbf{U}_j \otimes \mathbf{U}_k)[I_j I_k] \quad .$$

Definição 2.16. Seja $L_j = \left\{(\mathbf{U}_{j_1}, I_{j_1}), \ldots, (\mathbf{U}_{j_p}, I_{j_p})\right\}$ o nível j de um Γ–circuito quântico C. O operador unitário realizado pelo nível j do circuito C é

$$\mathbf{L}_j = \mathbf{U}_{j_1}[I_{j_1}] \cdots \mathbf{U}_{j_p}[I_{j_p}] \,.$$

Teorema 2.7. Seja $L_j = \left\{(\mathbf{U}_{j_1}, I_{j_1}), \ldots, (\mathbf{U}_{j_p}, I_{j_p})\right\}$ o nível j de um Γ–circuito quântico C. Então o operador realizado por L_j é idêntico, a menos de uma permutação, à extensão a $\mathcal{H}(\Gamma)$ do produto tensorial $\mathbf{U}_{j_1} \otimes \cdots \otimes \mathbf{U}_{j_p}$.

Demonstração. Obtém-se por indução utilizando o lema 2.1. □

Encerra-se esta secção de análise e especificação formal dos conceitos de circuito quântico e respectivo grafo associado enunciando o seguinte resultado geral, cuja demonstração é uma simples consequência do até então exposto.

Teorema 2.8. Seja C um Γ–circuito quântico de profundidade k. Então é possível escrever o operador $\mathbf{U}$ realizado pelo circuito C na forma

$$\mathbf{U} = \mathbf{L}_k \cdot \mathbf{L}_{k-1} \cdots \mathbf{L}_1 \,,$$

onde $\mathbf{L}_i$ designa o operador unitário realizado pelo nível i do circuito, $i \in [1 \,..\, k]$.

2.4.2 Realização de operadores por circuitos quânticos

Pela definição 2.12 cada Γ–circuito quântico realiza um operador $\mathbf{U} \in \mathcal{U}(\Gamma)$. Cada circuito C pode ser encarado como uma máquina abstracta, veja-se a figura 2.7, a qual uma vez inicializada no estado $|\phi\rangle \in \mathcal{H}(\Gamma)$ produz o estado $|\psi\rangle = \mathbf{U}|\phi\rangle \in \mathcal{H}(\Gamma)$.

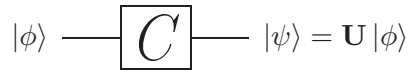


Figura 2.7: Realização de um operador por um circuito.

Mais geralmente, na implementação de um operador unitário por um circuito quântico é conveniente considerar um espaço de trabalho auxiliar. Atribui-se a alguns dos qudits do circuito um caracter temporário cujo estado final não é importante para a funcionalidade do operador implementado. Esses qudits designam-se *qudits ancilares* ou simplesmente *ancilas* e o espaço de Hilbert subjacente constitui o *espaço ancilar*. Os restantes qudits do sistema são *qudits principais* e o espaço de Hilbert subjacente designa-se *espaço principal*.

Para que as estatísticas resultantes da medição do estado final dos qudits principais do sistema quântico sejam independentes do estado dos qudits ancilares é fundamental que não exista correlação entre os sistemas. Dito de outro modo, antes de uma qualquer medição deve garantir-se o não entrelaçamento entre os sistemas principal e ancilar.

Uma forma expedita de assegurar, antes de uma medição, a não correlação entre os estados dos sistemas principal e ancilar consiste em estender o circuito com níveis que incluem, pela ordem inversa, as portas quânticas inversas de todas as portas que afectam o sistema ancilar. Assim, se o estado inicial dos qudits ancilares é um estado base particular, por exemplo $|0\rangle$, então o seu estado final será também $|0\rangle$ e esses qudits são reutilizáveis em operações subsequentes (em outros circuitos).

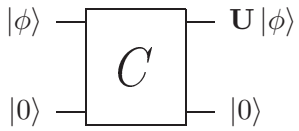


Figura 2.8: Realização de um operador por um circuito com ancilas.

No que se segue considera-se em cada linguagem Γ uma palavra específica denotada por 0. A palavra 0 de uma qualquer linguagem produto Γ de comprimento n é dada pela concatenação das palavras $0 \in \Gamma_1$, $0 \in \Gamma_2$, $\ldots$, $0 \in \Gamma_n$.

Definição 2.17. Considerem-se os conjuntos de índices $J \subset I$, $K = I \setminus J$ e uma linguagem produto $\Gamma = \Gamma_I$. Diz-se que um operador $\mathbf{U} \in \mathcal{U}(\Gamma_J)$ é realizado por um Γ–circuito quântico

usando espaço ancilar $\mathcal{H}(\Gamma_K)$ se o operador realizado pelo circuito, $\mathbf{W} \in \mathcal{U}(\Gamma)$, preserva o subespaço de $\mathcal{H}(\Gamma)$ onde o estado dos qudits ancilares é $|0\rangle$ e se nesse subespaço é, a menos de uma permutação, idêntico a $\mathbf{U} \otimes \mathbf{I}_{\Gamma_K}$.

Observação 2.4. Considere-se na definição anterior a permutação $\boldsymbol{\pi}$ de I definida por $\boldsymbol{\pi}(I) = JK$. Então para $|\phi\rangle \in \mathcal{H}(\Gamma_J)$ o operador $\mathbf{W}$ satisfaz

$$\mathbf{P}_{\boldsymbol{\pi}}\mathbf{W}\mathbf{P}_{\boldsymbol{\pi}}^{\dagger}(|\phi\rangle \otimes |0\rangle) = (\mathbf{U}|\phi\rangle) \otimes |0\rangle \quad ,$$

onde $|0\rangle \in \mathcal{H}(\Gamma_K)$. A figura 2.8 ilustra a acção de um tal circuito.

Uma vez que, por definição, os conceitos de porta quântica e operador unitário são equivalentes, a realização de portas quânticas por circuitos quânticos traduz a noção de decomposição de um operador unitário num produto de operadores unitários com acção local.

O conceito de realização introduzido na definição anterior é de realização exacta. A realização aproximada de operadores por circuitos obtém-se definindo uma norma no espaço dos operadores unitários, a qual por sua vez permite definir o erro de um circuito quântico (do operador realizado pelo circuito) na realização de um operador unitário. Um resultado fundamental para sistemas de qubits é o Teorema de Solovay-Kitaev o qual estabelece o grau de convergência na realização aproximada de um operador por circuitos quânticos baseados num conjunto finito de portas quânticas [33].

2.4.3 Circuitos quânticos reconhecedores de linguagens

Definição 2.18. Um $(\Gamma, \mathrm{In}, \mathrm{Out})$–circuito quântico é um terno $(C, \mathrm{In}, \mathrm{Out})$ onde C é um Γ-circuito quântico e In e Out são conjuntos de índices $\mathrm{In}, \mathrm{Out} \subseteq [1 \,..\, \mathrm{comp}(\Gamma)]$.

As *linguagens de entrada e saída* de um $(\Gamma, \mathrm{In}, \mathrm{Out})$–circuito quântico são, respectivamente, Γ_{In} e Γ_{Out}.

A cada circuito quântico associa-se um Γ-registo quântico $R = (\psi, I)$ de forma que, considerando $I = \left[i_1 \,..\, i_{\mathrm{comp}(\Gamma)}\right]$, o j-ésimo fio quântico no circuito corresponde ao Γ_{i_j}–qudit ψ_{i_j} do registo R. Assim, R_{In} denota o *registo de entrada* do circuito dado pelo subregisto de R constituído pelos qudits $\{\psi_i : i \in I_{\mathrm{In}}\}$ e o *registo de saída* do circuito corresponde ao subregisto R_{Out} de R constituído pelos qudits $\{\psi_i : i \in I_{\mathrm{Out}}\}$.

A funcionalidade de um circuito quântico, ilustrada na figura 2.9, consiste no seguinte processo: Inicialmente prepara-se o registo de entrada num estado $|x\rangle$ correspondente a uma dada palavra $x \in \Gamma_{\mathrm{In}}$ enquanto o registo constituído pelos restantes qudits, $\{\psi_i : i \in I \backslash I_{\mathrm{In}}\}$, é inicializado no estado $|0\rangle$. Assim, a menos de uma permutação, o estado inicial do sistema quântico subjacente ao registo R é $|x\rangle \otimes |0\rangle$. Após a evolução unitária prescrita pelo operador realizado pelo circuito, efectua-se uma medição do registo de saída na base computacional, a qual terá como resultado uma certa palavra $y \in \Gamma_{\mathrm{Out}}$.

Denota-se por $\mathrm{prob}_C(y \mid x)$ a probabilidade de observar $y \in \Gamma_{\mathrm{Out}}$ pela medição do registo de saída de um circuito quântico dado que o registo de entrada é inicializado com $x \in \Gamma_{\mathrm{In}}$.

Seja $|\psi\rangle = \sum_{s\in\Gamma} \alpha_s |s\rangle$ o estado do registo R associado ao circuito C após a acção do operador unitário $\mathbf{U}_C$ realizado pelo circuito e antes da medição final. Note-se que $|\psi\rangle = \mathbf{U}_C \left|\boldsymbol{\pi}_{\mathrm{In}}^{-1}(x, 0)\right\rangle$ onde $\boldsymbol{\pi}_{\mathrm{In}}$ é a permutação de I tal que $\boldsymbol{\pi}_{\mathrm{In}}(I) = I_{\mathrm{In}} \times (I \setminus I_{\mathrm{In}})$. Seja $\boldsymbol{\pi}_{\mathrm{Out}}$ a permutação de I tal que $\boldsymbol{\pi}_{\mathrm{Out}}(I) = I_{\mathrm{Out}} \times (I \setminus I_{\mathrm{Out}})$. De acordo com o teorema 2.5 a probabilidade de observar y dada a entrada x é

$$\mathrm{prob}_C(y \mid x) = \sum_{u \in \Gamma_{I \setminus I_{\mathrm{Out}}}} \left| \alpha_{\boldsymbol{\pi}_{\mathrm{Out}}^{-1}(yu)} \right|^2 \quad .$$

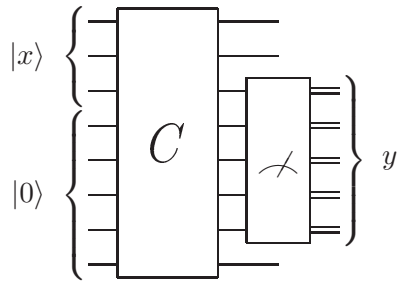


Figura 2.9: Funcionalidade de um circuito quântico.

Observação 2.5. No que se segue, faz-se uso da notação $\Gamma^{(n)}$ para indicar que existem n linguagens $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ tais que $\Gamma^{(n)} = \Gamma_1\Gamma_2\cdots\Gamma_n$ isto é que $\Gamma^{(n)}$ é uma linguagem produto de n linguagens. *À priori* não se assume a validade da recorrência $\Gamma^{(n+1)} = \Gamma^{(n)}\Gamma_{n+1}$ embora esta seja verdadeira em sistemas de qubits ou mais geralmente em sistemas não híbridos (todos os qudits do sistema definidos sobre a mesma linguagem).

Uma família de circuitos quânticos é uma sucessão $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$ em que C_n é um

$(\Gamma(n), \mathrm{In}(n), \mathrm{Out}(n))$– circuito quântico.

Para $n \in \mathbb{N}$, $\Gamma_{\mathrm{In}}^{(n)}$ representa a linguagem de entrada do n-ésimo circuito da família, i.e., $\Gamma_{\mathrm{In}}^{(n)} = \Gamma(n)_{\mathrm{In}(n)}$. A linguagem de entrada da família $\mathcal{C}$ de circuitos quânticos define-se[5] por

$$\Gamma_{\mathrm{In}}^{(*)} = \bigcup_{n \in \mathbb{N}} \Gamma_{\mathrm{In}}^{(n)} \quad .$$

Seja C um $(\Gamma, \mathrm{In}, \mathrm{Out})$–circuito quântico e $\{0,1\} \subseteq \Gamma_{\mathrm{Out}}$. Para $x \in \Gamma_{\mathrm{In}}$ diz-se que C aceita x com probabilidade p se $\mathrm{prob}_C(1 \mid x) = p$. Diz-se que rejeita x com probabilidade p se $\mathrm{prob}_C(0 \mid x) = p$.

Diz-se que C reconhece uma linguagem $L \subseteq \Gamma_{\mathrm{In}}$ com probabilidade pelo menos p se C aceita x com probabilidade pelo menos p para $x \in L$ e se rejeita x com probabilidade pelo menos p para $x \notin L$.

Diz-se que uma família de circuitos quânticos $\mathcal{C} = \{C_n\}_{n \in \mathbb{N}}$ reconhece uma linguagem $L \subseteq \Gamma_{\mathrm{In}}^{(*)}$ com probabilidade pelo menos p se $\forall n \in \mathbb{N}$, C_n reconhece a linguagem $L_n = L \cap \Gamma_{\mathrm{In}}^{(n)}$ com probabilidade pelo menos p.

Diz-se que $\mathcal{C}$ reconhece uma linguagem $L \subseteq \Gamma_{\mathrm{In}}^{(*)}$ com probabilidade uniformemente superior a p se existe uma constante $0 < \delta \leq 1 - p$ tal que $\forall n \in \mathbb{N}$, C_n reconhece L_n com probabilidade pelo menos $p + \delta$.

As definições anteriores permitem considerar classes de linguagens reconhecidas por classes de famílias de circuitos quânticos e assim alicerçar uma teoria da Complexidade de Circuitos Quânticos em sistemas de Γ–qudits. Nesse sentido é ainda imperativo fixar um conjunto de portas quânticas base.

Definição 2.19. Seja $\mathcal{G}$ um conjunto de operadores unitários em $\Gamma^{(*)}$. Diz-se que um operador unitário $\mathbf{U}$ é realizável por um circuito quântico com base num conjunto de portas quânticas $\mathcal{G}$ se existe um circuito quântico $K = (\mathbf{U}_1, I_1), (\mathbf{U}_2, I_2), \ldots, (\mathbf{U}_m, I_m)$ que realiza $\mathbf{U}$ e tal que $\mathbf{U}_i \in \mathcal{G}$, $i = 1, \ldots, m$.

Os elementos de $\mathcal{G}$ designam-se portas base.

O tamanho do menor circuito quântico com base $\mathcal{G}$ que realiza um dado operador $\mathbf{U}$ designa-se por tamanho de $\mathbf{U}$ em $\mathcal{G}$.

[5] A definição é análoga à linguagem de fecho de Kleene em linguagens formais. No entanto a linguagem $\Gamma_{\mathrm{In}}^{(*)}$ não inclui a palavra vazia, o que corresponderia a ter na família $\mathcal{C}$ um circuito sem entradas.

A definição anterior foi colocada em termos de realização de operadores. É possível considerar-se uma definição análoga para reconhecimento de linguagens.

Se por um lado o conjunto constituído pelas portas de Rotação de Givens (com ângulo θ computável) e pelas portas de Controlo de Muthukrishnan-Stroud, referidas na secção 2.2, é candidato a conjunto (infinito) exactamente universal para computação em sistemas de Γ–qudits, por outro encontra-se em aberto o problema de determinar um conjunto finito de portas quânticas aproximadamente universal.

Um outro aspecto é a questão da uniformidade dos circuitos. Sabe-se, no contexto dos circuitos booleanos clássicos, ser necessário introduzir uma noção de uniformidade de circuitos para que o modelo seja razoável (i.e., de modo a inibir a possibilidade de uma família de circuitos decidir linguagens não decidíveis pelas máquinas de Turing). Para sistemas de qubits, só recentemente se esclareceram as questões da uniformidade e equivalência entre os modelos de máquinas de Turing quânticas e famílias de circuitos quânticos.

Considere-se uma linguagem $L \subseteq \{0,1\}^*$. Diz-se que

- L pertence à classe de complexidade $L \in \mathbf{EQP}$ (exact quantum polinomial time) se existe uma máquina de Turing quântica que em tempo polinomial reconhece L com probabilidade 1 (reconhece a linguagem de forma exacta);

- L pertence à classe de complexidade **BQP** (bounded probabilistic quantum polinomial time) se existe uma máquina de Turing quântica, M, que em tempo polinomial reconhece L com probabilidade uniformemente superior a $1/2$;

- L pertence à classe de complexidade **ZQP** (zero error quantum polinomial time) se existe uma máquina de Turing quântica, M, que em tempo polinomial reconhece L com probabilidade uniformemente superior a $1/2$ e para além disso satisfaz as condições seguintes:

  1. se M aceita x com probabilidade não nula então rejeita x com probabilidade 0;
  2. se M rejeita x com probabilidade não nula então aceita x com probabilidade 0.

Em 2000, Kitaev e Watrous [34] definiram um modelo de famílias de circuitos quânticos uniformemente gerados em tempo polinomial e baseados num conjunto de 5 portas quânti-

cas, a base de Shor, equivalente a **BQP**. Este modelo é apenas adequado no contexto de reconhecimento probabilístico de linguagens, uma vez que no caso exacto as famílias de circuitos uniformemente gerados em tempo polinomial reconhecem a classe **P** em vez de **EQP** [40]. Por outro lado, removendo a restrição no número de portas quânticas base obtém-se o modelo das famílias de circuitos quânticos uniformes. Mostra-se que esta classe reconhece precisamente **BQP** mas, no casos exacto e de erro zero, reconhecem mais do que deveriam. De facto, mostra-se que neste modelo é possível construir uma família de circuitos quânticos que implementa de forma exacta a transformada quântica de Fourier de qualquer ordem, um problema não resolúvel de forma exacta por máquinas de Turing Quânticas [36], [43]. A questão da uniformidade foi finalmente resolvida por Nishimura e Ozawa [42] ao estabelecerem uma equivalência perfeita entre máquinas de Turing quânticas e um modelo de famílias de circuitos quânticos uniformes finitamente gerados.

Qualquer modelo razoável de Γ–circuitos uniformes deverá ter em consideração que o número de diferentes tipos de qudits deve ser finito, caso contrário poder-se-ia codificar a informação não computável na dimensão do espaço de estados dos sistemas físicos subjacentes. Neste modelo, é necessário ainda formalizar um conceito adequado de famílias de circuitos uniformes finitamente gerados. A formalização destes conceitos encontra-se numa fase inicial de investigação bem como o consequente estudo da relação entre os modelos de Computação Quântica baseados em qubits, qudits e Γ–qudits. Conjectura-se no entanto que o poder computacional destes três modelos será equivalente, i.e., a classe **BQP** será equivalente à classe de famílias de circuitos quânticos uniformes finitamente gerados em qualquer dos modelos.

2.5 Paralelização de operadores quânticos

Em 1998, Moore e Nilsson [35] demonstraram ser possível realizar qualquer permutação de estados de qubits usando circuitos quânticos de profundidade constante. O teorema seguinte generaliza aqueles resultados para o caso de uma permutação arbitrária de n Γ–qudits:

Teorema 2.9. Sejam Γ uma linguagem e $\boldsymbol{\pi}$ uma permutação de $[1 \,..\, n]$, com $n \geq 2$. Então o operador de permutação $\mathbf{P}_{\boldsymbol{\pi}} : \mathcal{H}(\Gamma^n) \rightarrow \mathcal{H}(\Gamma^n)$ é realizável por um circuito quântico com n Γ-qudits ancilares, tamanho $4n$ e profundidade 4.

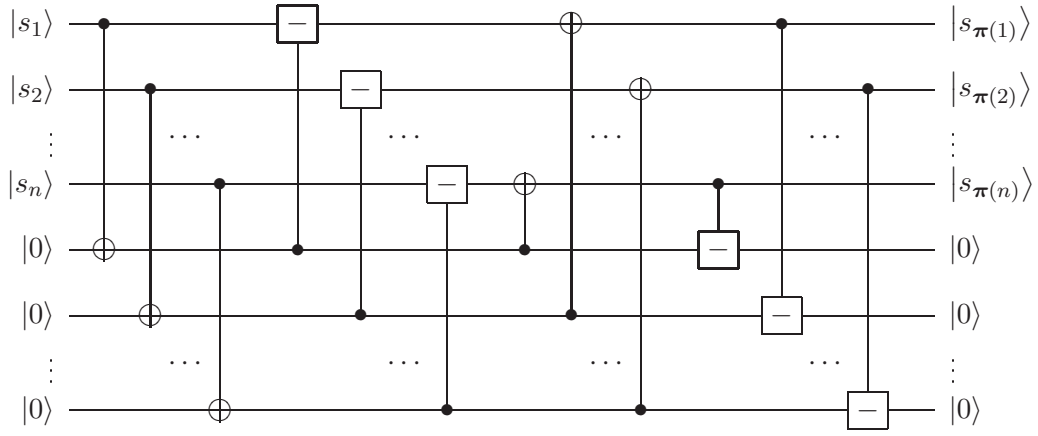


Figura 2.10: Realização com ancilas de uma permutação do estado n qudits.

Demonstração. Realiza-se uma cópia do estado dos n qudits principais para um registo ancilar. Usando as ancilas, colocam-se os qudits principais no estado $|0\rangle$. Copiam-se os estados dos qudits ancilares para os qudits principais na ordem induzida pela permutação. Finalmente repõe-se o estado das ancilas a $|0\rangle$. As portas quânticas utilizadas em cada um dos passos anteriores podem ser aplicadas em paralelo, pelo que a profundidade do circuito é constante e igual a 4 como se ilustra na figura 2.10. □

É possível eliminar a utilização de qudits ancilares aumentando ligeiramente a profundidade do circuito, como mostra o próximo resultado.

Teorema 2.10. Sejam Γ uma linguagem e $\boldsymbol{\pi}$ uma permutação de $[1 \,..\, n]$, com $n \geq 2$. Então o operador de permutação $\mathbf{P}_{\boldsymbol{\pi}} : \mathcal{H}(\Gamma^n) \to \mathcal{H}(\Gamma^n)$ é realizável por um circuito quântico sem ancilas e com profundidade constante.

Demonstração. Sabe-se que qualquer permutação se pode escrever como a composição de ciclos disjuntos. Por sua vez, é possível decompor cada ciclo num produto de dois conjuntos disjuntos de transposições que se obtém por duas quaisquer reflexões geradoras do grupo de simetrias do ciclo. Cada transposição é realizada pelo operador de troca representado na figura 2.11. (Recorrendo ao operador de soma e a uma generalização da porta de Hadamard, o operador de troca é realizável sem ancilas, [13].) □

Exemplo 2.1. Considere-se a permutação $\boldsymbol{\pi}$ de $[1 \,..\, 8]$ dada por $[2, 4, 5, 7, 6, 3, 8, 1]$. A decomposição de $\boldsymbol{\pi}$ em ciclos disjuntos é $(1\,2\,4\,7\,8)(3\,5\,6)$. Ao primeiro dos ciclos, representado

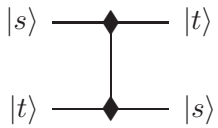


Figura 2.11: Acção da porta quântica **SWAP**

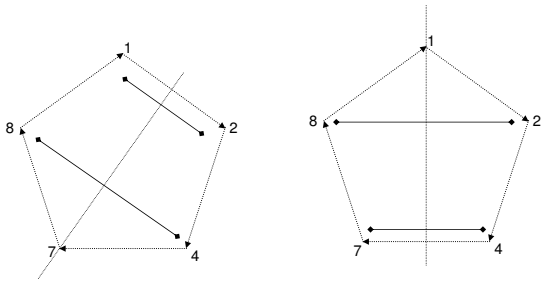


Figura 2.12: Decomposição de um ciclo num produto de transposições.

na figura 2.12, corresponde o produto das transposições $(1\,2)(4\,8)$ e $(2\,8)(4\,7)$. A decomposição do ciclo $(3\,5\,6)$ obtém-se de forma análoga como o produto das transposições $(3\,5)$ e $(5\,6)$. A figura 2.13 ilustra o circuito quântico correspondente.

Recentemente, têm-se alcançado progressos significativos na compreensão do poder de famílias quânticas de circuitos com profundidade constante, [22][26][23][29]. Os interessantes resultados obtidos permitiram diferenciar certas classes de complexidade no modelo de circuitos com qubits das correspondentes classes no modelo clássico.

Estes resultados apoiam-se na hipótese de realizar em profundidade constante a porta de

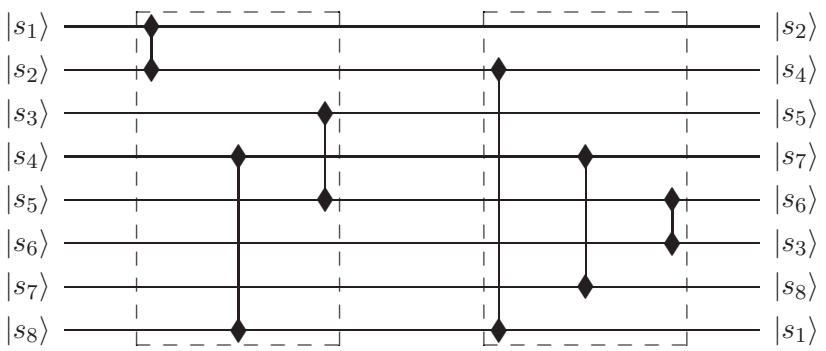


Figura 2.13: Realização sem ancilas da permutação $\boldsymbol{\pi}$ do exemplo 2.1.

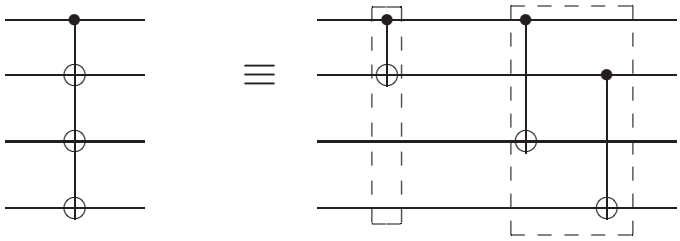


Figura 2.14: A porta de *fanout*

fanout, a qual realiza cópias (na base computacional) do estado de um qubit para n qubits. Note-se que este pressuposto é tido como garantido no modelo Clássico de circuitos booleanos, mesmo em classes de complexidade que limitam o grau de entrada de cada porta num circuito booleano (e.g., a classe **NC**).

Usando a porta quântica de cópia, demonstra-se facilmente que é possível realizar n cópias de um Γ-qudit em profundidade $\mathcal{O}(\log n)$, como se ilustra na figura 2.14. A porta de *fanout* é definida por

$$\mathbf{FANOUT} : \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma^n) \rightarrow \mathcal{H}(\Gamma) \otimes \mathcal{H}(\Gamma^n)$$

$$\mathbf{FANOUT}\,|s\rangle\,|t_1\rangle\,|t_2\rangle \cdots |t_n\rangle = |s\rangle\,|(s+t_1) \bmod \Gamma\rangle\,|(s+t_2) \bmod \Gamma\rangle \cdots |(s+t_n) \bmod \Gamma\rangle\ .$$

Em Høyer e Špalek [29] demonstra-se o poder da porta de *fanout* para a construção de circuitos com profundidade constante, no modelo de computação com qubits. Entre outras mostra-se a possibilidade de aproximar com profundidade constante o equivalente quântico da porta de *limiar*, o que permite, com base em resultados estabelecidos na área da Computação Clássica em Redes Neuronais, realizar de forma aproximada todas as operações aritméticas por circuitos quânticos com profundidade constante.

Encontra-se em estudo a forma como estes resultados se adaptarão ao modelo de computação com Γ–qudits.

Adição em Tempo Constante $\langle \mathbf{3}|$

Na sua esmagadora maioria, os trabalhos de investigação sobre aritmética em Computação Quântica aplicam-se a sistemas de qubits. O caso da adição não é excepção.

Num trabalho pioneiro de 1995, Vedral et al. [52] apresentam um circuito quântico para somar dois números de n bits com profundidade $3n$ e que utiliza $n+1$ qubits ancilares. Em 1998, Gossett [25] apresenta um circuito quântico para a adição de k números de n bits, baseado na técnica de guarda de transporte, com profundidade $4 \log k$ e tamanho $4nk$. Em 2000, Draper [18] apresenta um somador quântico, baseado na transformada quântica de Fourier, de profundidade linear, mas com a particularidade de não utilizar qubits ancilares. Em 2004, o mesmo autor [19] apresenta um circuito quântico baseado na técnica de "carry-lookahead" com profundidade $2 \log n$ e que utiliza $n - \log n$ qubits ancilares.

Neste capítulo estuda-se o problema da adição de números, representados por sequências de dígitos, em sistemas de representação redundantes.

Consideram-se versões quânticas de dois algoritmos clássicos de adição originalmente descritos por Parhami [44]. As duas classes de circuitos quânticos obtidas, com profundidade constante e tamanho linear, cobrem todos os sistemas de representação redundantes. Concretiza-se ainda o circuito quântico para o sistema redundante de representação $\mathrm{GSD}(3, 3, 4)$.

O desenvolvimento de algoritmos quânticos eficientes para a resolução do problema da adição de m números com n dígitos tem assaz importância já que este se relaciona directamente com os problemas da multiplicação e divisão de números. Pela primeira vez, de uma forma unificada, estabelecem-se condições necessárias e suficientes para a aplicação de um algoritmo para a soma de m números, num sistema redundante de representação, sem propagação de

dígitos de transporte, configurando-se assim a possibilidade de definir circuitos quânticos com profundidade constante para resolver o problema da adição de m números de n dígitos.

Os circuitos aqui descritos pertencem à família de circuitos quânticos híbridos e constituem uma particularização do modelo geral de circuitos em sistemas de Γ-qudits estabelecido no capítulo 2.

Definição 3.1. Sejam $r \geq 2$, $\alpha, \beta \geq 0$ inteiros tais que $\alpha+\beta \geq r-1$. Um *sistema generalizado de representação*, $\mathrm{GSD}(r, \alpha, \beta)$, é um sistema posicional de raiz r com conjunto de dígitos $\{-\alpha, \ldots, \beta\}$.

Definição 3.2. Seja $\mathcal{N} = \mathrm{GSD}(r, \alpha, \beta)$ um sistema generalizado de representação.

O *factor negativo de redundância* de $\mathcal{N}$ é $\rho^- = \frac{\alpha}{r-1}$.

O *factor positivo de redundância* de $\mathcal{N}$ é $\rho^+ = \frac{\beta}{r-1}$.

O *factor de redundância* de $\mathcal{N}$ é $\rho = \rho^- + \rho^+ = \frac{\alpha+\beta}{r-1}$.

Definição 3.3. Seja $\mathcal{N} = \mathrm{GSD}(r, \alpha, \beta)$ um sistema generalizado de representação. Diz-se que $\mathcal{N}$ é um *sistema redundante* se $\rho > 1$. Caso contrário, i.e., se $\rho = 1$, diz-se que $\mathcal{N}$ é um *sistema não redundante*.

No que se segue, para um dado sistema de representação $\mathcal{N} = \mathrm{GSD}(r, \alpha, \beta)$, $\mathcal{H}_\mathcal{N}$ denota o espaço de Hilbert com a base computacional constituída pelos kets $|s\rangle$, $s \in \{-\alpha, \ldots, \beta\}$. O conjunto dos operadores unitários em $\mathcal{H}_\mathcal{N}$ denota-se por $\mathcal{U}(\mathcal{H}_\mathcal{N})$.

3.1 Adição de dois inteiros

A adição de dois inteiros $x \equiv x_{n-1} \cdots x_1 x_0$ e $y \equiv y_{n-1} \cdots y_1 y_0$ consiste, essencialmente, em separar $x_i + y_i$ num dígito soma parcial w_i e num dígito de transporte para a posição seguinte, c_{i+1}. Geralmente, c_{i+1} é função não só de x_i e y_i mas também do dígito de transporte c_i. Assim, para calcular c_{i+1} é necessário aguardar pelo cálculo de c_i ou considerar c_{i+1} função de todos os dígitos x_j e y_j para $j \leq i$. O desenvolvimento de métodos que permitam limitar a propagação de dígitos de transporte constitui um factor decisivo na redução da complexidade linear do algoritmo convencional para a adição.

Uma importante característica dos algoritmos a seguir apresentados é a possibilidade de estes serem totalmente paralelizáveis na forma de circuitos com profundidade constante.

Considere-se um sistema de representação $\mathcal{N} = \text{GSD}(\alpha, \beta, r)$. Dados dois inteiros x e y, representados por sequências de n dígitos, pretende-se determinar uma representação em $\mathcal{N}$ para o inteiro $z = x + y$. Denote-se este problema por $\mathbf{Soma}_{\mathcal{N}}(n)$.

O algoritmo de Adição sem Propagação de Dígitos de Transporte (CFA) consiste em determinar, numa primeira fase, as somas parciais, w_i, e os dígitos de transporte, c_{i+1}, como função de x_i e y_i. Numa segunda fase calculam-se os dígitos soma final, z_i, pela simples adição das somas parciais, w_i, e dos dígitos de transporte, c_i. Os dígitos de transporte e somas parciais gerados na primeira fase devem permitir a absorção de cada dígito de transporte para a posição i no cálculo da soma final $z_i = w_i + c_i$, i.e., $z_i \in S(\mathcal{N})$, $i = 0, \ldots, n-1$.

Algoritmo 3.1. Adição sem Propagação de Dígitos de Transporte (CFA) para a resolução do problema $\mathbf{Soma}_{\mathcal{N}}(n)$:

```
PARA i DESDE 0 ATÉ n-1
  calcular c[i+1] e w[i] usando x[i] e y[i];
PARA i DESDE 0 ATÉ n-1
  calcular z[i] usando w[i] e c[i].
```

A classe de sistemas redundantes de representação que suportam o algoritmo CFA, foi originalmente identificada por Parhami [44].

Teorema 3.1 (Parhami [44], Pereira [45])**.** Seja ρ o coeficiente de redundância de um sistema de representação $\mathcal{N} = \text{GSD}(\alpha, \beta, r)$. O algoritmo 3.1 é aplicável ao problema $\mathbf{Soma}_{\mathcal{N}}(n)$ se e só se ($\rho \geq 1 + \frac{3}{r-1}$ e $r > 2$) ou ($\rho = 1 + \frac{2}{r-1}$, $\alpha \neq 1$ e $r > 2$) ou ($\rho = 1 + \frac{2}{r-1}$, $\beta \neq 1$ e $r > 2$).

No algoritmo de Propagação Limitada de Dígitos de Transporte (LCPA) são inicialmente determinadas estimativas binárias, e_{i+1}, para os dígitos de transporte c_{i+1}, em função dos dígitos x_i e y_i. Numa segunda fase determinam-se as somas parciais, w_i, e os dígitos de transporte c_{i+1} como função de x_i, y_i e e_i. A última fase consiste em calcular os dígitos soma final, z_i, por simples adição das somas parciais, w_i, e dos dígitos de transporte, c_i. Os dígitos estimativa, de transporte e soma parcial são gerados de modo a permitir a absorção

total de cada dígito de transporte para a posição i no cálculo da soma final $z_i = w_i + c_i$, i.e., $z_i \in S(\mathcal{N})$, $i = 0, \ldots, n-1$.

Como se mostra em Parhami [44] ou Pereira [45] o algoritmo LCPA é aplicável a qualquer sistema de representação redundante.

Algoritmo 3.2. Adição com Propagação Limitada de Dígitos de Transporte (LCPA)

```
PARA i DESDE 0 ATÉ n-2
  calcular e[i+1] usando x[i] e y[i];
PARA i DESDE 0 ATÉ n-1
  calcular c[i+1] e w[i] usando x[i], y[i] e e[i];
PARA i DESDE 0 ATÉ n-1
  calcular z[i] usando w[i] e c[i].
```

Definem-se em seguida os circuitos quânticos QCFA e QLCPA que implementam, respectivamente, os algoritmos 3.1 e 3.2. A funcionalidade dos circuitos apresentados consiste na composição de operadores unitários com acção local sobre o espaço de Hilbert subjacente aos registos quânticos das entradas $|x\rangle$ e $|y\rangle$, do resultado $|z\rangle$ e de algum espaço ancilar. Os estados dos qudits ancilares, quer à entrada, quer à saída do circuito são idênticos a $|0\rangle$.

Se se ignorar o espaço ancilar, cada circuito para o problema $\mathbf{Soma}_{\mathcal{N}}(n)$ implementa um operador unitário $\mathbf{U}$ que deverá satisfazer,

$$\mathbf{U}\,|x\rangle\,|y\rangle\,|0\rangle = |x\rangle\,|y\rangle\,|x+y\rangle \quad , \tag{3.1}$$

em que $|x\rangle, |y\rangle \in \mathcal{H}_{\mathcal{N}}^{\otimes n}$ são dois registos que contêm as representações em n qudits dos inteiros x e y. $|0\rangle \in \mathcal{H}_{\mathcal{N}}^{\otimes(n+1)}$ é o estado inicial do registo z.

3.1.1 O circuito QCFA para o problema $\mathbf{Soma}_{\mathcal{N}}(n)$

Cada dígito de transporte no Algoritmo 3.1 é calculado com a avaliação de uma função $c : S(\mathcal{N})^2 \to S_c$ em que $S_c = \{-\lambda, \ldots, \mu\}$ é o conjunto dos possíveis dígitos de transporte. A função c depende apenas do sistema de representação $\mathcal{N}$ (veja-se Parhami [44] ou Pereira [45]).

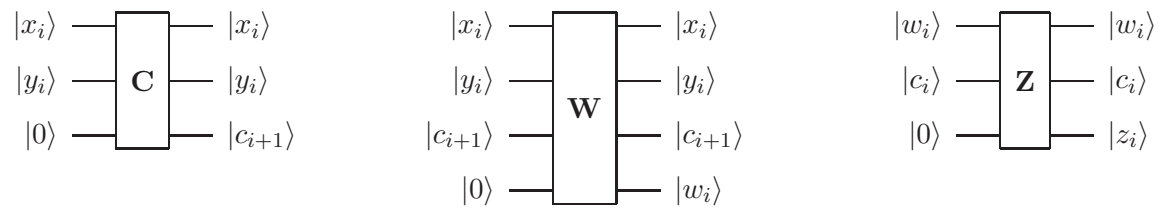


Figura 3.1: As portas quânticas **C**, **W** e **Z** para o circuito QCFA

Definição 3.4. Sejam a e b inteiros não negativos tais que $d = a + b \geq 1$ e seja $S = [-a \,..\, b]$. Para qualquer inteiro n, o resíduo módulo S de n denota-se por $n \bmod S$ e é igual ao único inteiro $m \in S$ que satisfaz $m + a = (n + a) \bmod d$.

Seja $\mathcal{N}_c = \mathrm{GSD}(\lambda, \mu, 2)$. Note-se que $S_c = S(\mathcal{N}_c)$. À função c corresponde o operador unitário $\mathbf{C} \in \mathcal{U}\left(\mathcal{H}_{\mathcal{N}}^{\otimes 2} \otimes \mathcal{H}_{\mathcal{N}_c}\right)$ definido por

$$\mathbf{C}\,|a\rangle\,|b\rangle\,|f\rangle = |a\rangle\,|b\rangle\,|(f + c(a,b)) \bmod S_c\rangle \tag{3.2}$$

e cuja acção é $\mathbf{C}\,|a\rangle\,|b\rangle\,|0\rangle = |a\rangle\,|b\rangle\,|c(a,b)\rangle$ (veja-se a figura 3.1).

O cálculo dos dígitos de transporte resulta da acção do operador unitário

$$\mathbf{L}_1 = \prod_{i=0}^{n-1} \mathbf{C}_{i+1} \equiv \mathbf{C}_n \mathbf{C}_{n-1} \cdots \mathbf{C}_2 \mathbf{C}_1 \ , \tag{3.3}$$

onde $\mathbf{C}_{i+1} = \mathbf{C}[x_i, y_i, c_{i+1}]$ para $i = 0, \ldots, n-2$ e $\mathbf{C}_n = \mathbf{C}[x_{n-1}, y_{n-1}, z_n]$. Note-se que os operadores $\mathbf{C}_i$ no produto (3.3) agem sobre conjuntos disjuntos de qudits, pelo que se podem aplicar em paralelo.

Observação 3.1. Note-se que o valor do dígito mais significativo da soma final, z_n, corresponde ao último dígito de transporte, c_n. Na realidade, a porta $\mathbf{C}_n$ em (3.3) não é exactamente igual $\mathbf{C}[x_{n-1}, y_{n-1}, z_n]$. De facto, geralmente, $\mathcal{N}_c \neq \mathcal{N}$ pelo que o qudit z_n é definido sobre um espaço de Hilbert diferente de $\mathcal{H}_{\mathcal{N}_c}$. No entanto $S(\mathcal{N}_c) \subset S(\mathcal{N})$. Assim $\mathbf{C}_n = \tilde{\mathbf{C}}[x_{n-1}, y_{n-1}, z_n]$, onde $\tilde{\mathbf{C}}$ é uma extensão unitária de $\mathbf{C}$ a $\mathcal{H}_{\mathcal{N}}$.

Sejam $S_w = \{-\alpha + \lambda, \ldots, \beta - \mu\}$ o conjunto dos possíveis dígitos soma parcial, $\mathcal{N}_w = \mathrm{GSD}(\alpha - \lambda, \beta - \mu, 2)$ e considere-se a função $w : S^2 \times S_c \to S_w$ definida por

$$w(a,b,c) = \begin{cases} a + b - r \cdot c & \text{se } c = c(a,b) \\ 0 & \text{caso contrário.} \end{cases} \tag{3.4}$$

Cada soma parcial resulta da aplicação do operador unitário $\mathbf{W} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}}^{\otimes 2} \otimes \mathcal{H}_{\mathcal{N}_c} \otimes \mathcal{H}_{\mathcal{N}_w})$ definido por

$$\mathbf{W} |a\rangle |b\rangle |c\rangle |g\rangle = |a\rangle |b\rangle |c\rangle |(g + w(a,b,c)) \bmod S_w\rangle \quad . \tag{3.5}$$

A acção deste operador, $\mathbf{W} |a\rangle |b\rangle |c\rangle |0\rangle = |a\rangle |b\rangle |c\rangle |w(a,b,c)\rangle$, ilustra-se na figura 3.1.

O cálculo em paralelo dos dígitos soma parcial consiste na aplicação do seguinte produto de operadores unitários

$$\mathbf{L}_2 = \prod_{i=0}^{n-1} \mathbf{W}_i \equiv \mathbf{W}_{n-1}\mathbf{W}_{n-2}\cdots\mathbf{W}_1\mathbf{W}_0 \ , \tag{3.6}$$

onde $\mathbf{W}_i = \mathbf{W}[x_i, y_i, c_{i+1}, w_i]$, $i = 0, \ldots, n-1$.

O cálculo de cada um dos dígitos soma final, z_i, $i = 0, 1, \ldots, n-1$, é realizado pela avaliação da função $z : S_w \times S_c \to S$ definida por $z(w,c) = w + c$. Associado a esta função define-se o operador unitário $\mathbf{Z} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}_w} \otimes \mathcal{H}_{\mathcal{N}_c} \otimes \mathcal{H}_{\mathcal{N}})$ por

$$\mathbf{Z} |w\rangle |c\rangle |h\rangle = |w\rangle |c\rangle |(h + z(w,c)) \bmod S\rangle \quad . \tag{3.7}$$

Na figura 3.1 ilustra-se a acção de $\mathbf{Z}$, $\mathbf{Z} |w\rangle |c\rangle |0\rangle = |w\rangle |c\rangle |w + c\rangle$.

Sejam $\mathbf{Z}_i = \mathbf{Z}[w_i, c_i, z_i]$, $i = 0, \ldots, n-1$. O cálculo em paralelo dos dígitos soma final é realizado pelo produto de operadores

$$\mathbf{L}_3 = \prod_{i=0}^{n-1} \mathbf{Z}_i \equiv \mathbf{Z}_{n-1}\mathbf{Z}_{n-2}\cdots\mathbf{Z}_1\mathbf{Z}_0 \ . \tag{3.8}$$

Após o cálculo dos dígitos soma final é necessário reverter o estado dos qudits dos registos de dígitos de transporte e de dígitos soma parcial ao seu estado inicial. Tal é alcançado pela aplicação em ordem inversa dos operadores que afectaram os qudits ancilares:

$$\mathbf{L}_4 = \mathbf{W}_0^\dagger \mathbf{W}_1^\dagger \cdots \mathbf{W}_{n-2}^\dagger \mathbf{W}_{n-1}^\dagger \ , \tag{3.9}$$

$$\mathbf{L}_5 = \mathbf{C}_1^\dagger \mathbf{C}_2^\dagger \cdots \mathbf{C}_{n-2}^\dagger \mathbf{C}_{n-1}^\dagger \ . \tag{3.10}$$

Sejam $\mathcal{H}_{\text{work}} = \mathcal{H}_{\mathcal{N}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}}^{\otimes n+1}$ o espaço principal e $\mathcal{H}_{\text{ancilla}} = \mathcal{H}_{\mathcal{N}_c}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}_w}^{\otimes n}$ o espaço ancilar utilizado pelo circuito QCFA. A este circuito corresponde o operador $\mathbf{V} \in \mathcal{U}(\mathcal{H}_{\text{work}} \otimes \mathcal{H}_{\text{ancilla}})$ definido por

$$\mathbf{V} = \mathbf{L}_5\mathbf{L}_4\mathbf{L}_3\mathbf{L}_2\mathbf{L}_1 \tag{3.11}$$

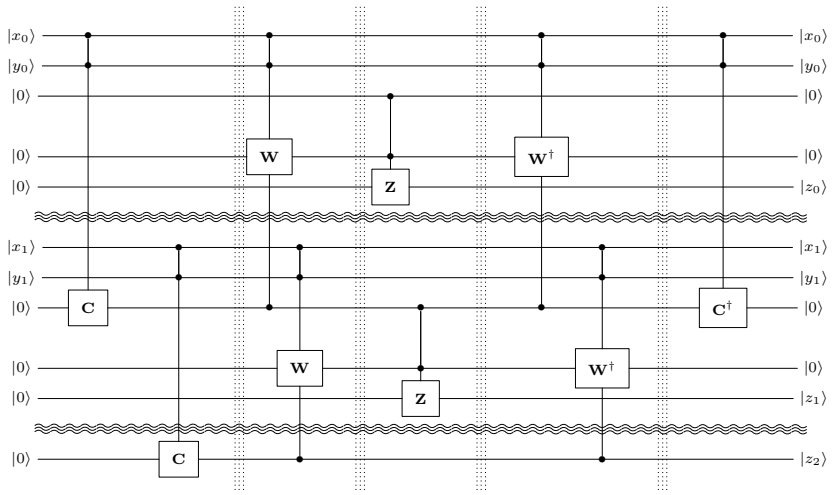


Figura 3.2: O circuito quântico QCFA para instâncias de tamanho $n = 2$

cuja acção é

$$\mathbf{V}(|x, y, z\rangle \otimes |0\rangle) = (\mathbf{U}\,|x, y, 0\rangle) \otimes |0\rangle \quad , \tag{3.12}$$

onde $\mathbf{U}$ é um operador com acção idêntica a (3.1).

Cada termo no produto (3.11) pode ser calculado em uma única unidade de tempo, já que as portas quânticas agem sobre conjuntos disjuntos de qudits. Assim, o circuito quântico QCFA para o problema $\mathbf{Soma}_{\mathcal{N}}(n)$ tem profundidade constante (igual a 5). O número total de portas $\mathbf{C}$, $\mathbf{W}$ e $\mathbf{Z}$ é linear $(5n - 1)$. A figura 3.2 ilustra o caso $n = 2$. As faixas verticais demarcam os 5 níveis do circuito. As linhas onduladas horizontais demarcam uma componente do circuito (qudits e portas quânticas) que, ao ser repetida, estende o circuito de forma a lidar com a adição de números de tamanho arbitrário.

3.1.2 O somador quântico LCPA

As estimativas binárias e_{i+1}, $i = 0, \ldots, n-2$, no Algoritmo 3.2 são calculadas como uma função $e : S(\mathcal{N})^2 \to \mathbb{B}$, $e(x_i, y_i) = e_{i+1}$. Esta função é extensível ao operador unitário $\mathbf{E} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}}^{\otimes 2} \otimes \mathcal{H}_2)$ definido por

$$\mathbf{E}\,|a\rangle\,|b\rangle\,|c\rangle = |a\rangle\,|b\rangle\,|c \oplus e(a, b)\rangle \quad , \tag{3.13}$$

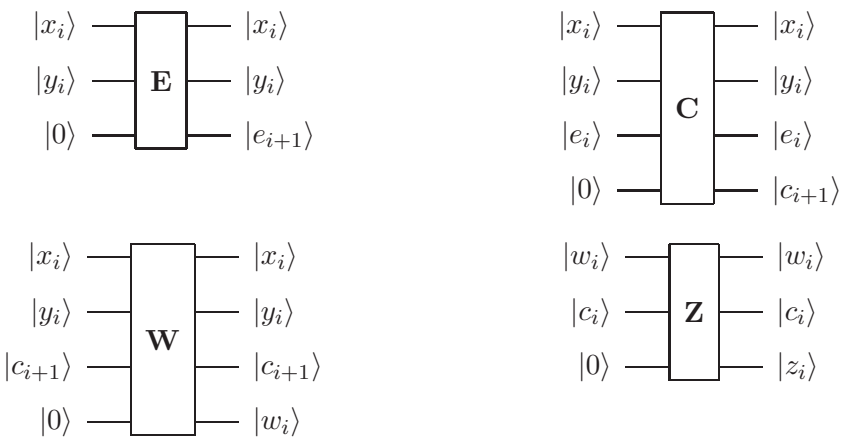


Figura 3.3: As portas quânticas **E**, **C**, **W** e **Z** para o circuito QLCPA

em que $\oplus$ denota a adição bit a bit módulo 2. A porta quântica associada a este operador, representada na figura 3.3, tem acção $\mathbf{E}\,|a\rangle\,|b\rangle\,|0\rangle = |a\rangle\,|b\rangle\,|e(a,b)\rangle$.

Seja $\mathbf{E}_{i+1} = \mathbf{E}[x_i, y_i, e_{i+1}]$, $i = 0, \ldots, n-2$. O cálculo das estimativas para os dígitos de transporte é dado pela acção do operador

$$\mathbf{L}_1 = \prod_{i=0}^{n-2} \mathbf{E}_{i+1} \equiv \mathbf{E}_{n-1}\mathbf{E}_{n-2}\cdots\mathbf{E}_2\mathbf{E}_1 \ . \tag{3.14}$$

Os operadores no produto (3.14) agem sobre conjuntos disjuntos de qudits, pelo que podem ser aplicados em simultâneo, i.e, as estimativas são calculadas em paralelo.

Seja $\mathcal{N}_c = \mathrm{GSD}(\lambda, \mu, 2)$. Cada dígito de transporte no algoritmo 3.2 é calculado como uma função $c : S(\mathcal{N})^2 \times \mathbb{B} \to S(\mathcal{N}_c)$ que depende apenas do sistema de representação $\mathcal{N}$. O operador unitário correspondente, $\mathbf{C} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}}^{\otimes 2} \otimes \mathcal{H}_2 \otimes \mathcal{H}_{\mathcal{N}_c})$ é definido por

$$\mathbf{C}\,|a\rangle\,|b\rangle\,|e\rangle\,|f\rangle = |a\rangle\,|b\rangle\,|e\rangle\,|(f + c(a,b,e)) \bmod S_c\rangle \ . \tag{3.15}$$

A acção de **C**, ilustrada na figura 3.3, é $\mathbf{C}\,|a\rangle\,|b\rangle\,|e\rangle\,|0\rangle = |a\rangle\,|b\rangle\,|e\rangle\,|c(a,b,e)\rangle$. O cálculo dos dígitos de transporte é realizada em paralelo pelo operador unitário

$$\mathbf{L}_2 = \prod_{i=0}^{n-1} \mathbf{C}_{i+1} \ , \tag{3.16}$$

onde $\mathbf{C}_{i+1} = \mathbf{C}[x_i, y_i, e_i, c_{i+1}]$, $i = 0, \ldots, n-2$. O dígito de transporte c_n torna-se no dígito mais significativo do registo z, i.e., $\mathbf{C}_n = \mathbf{C}[x_{n-1}, y_{n-1}, e_{n-1}, z_n]$. Veja-se a observação 3.1.

Seja $w : S(\mathcal{N})^2 \times S(\mathcal{N}_c) \to S(\mathcal{N}_w)$ a função definida por

$$w(x,y,c) = \begin{cases} x + y - r \cdot c & \text{se } c \in c^{-1}(S(\mathcal{N})^2 \times \mathbb{B}) \\ 0 & \text{caso contrário.} \end{cases} \tag{3.17}$$

O cálculo de cada soma parcial w_i, $i = 0, \ldots, n-1$, é realizado pela acção do operador $\mathbf{W} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}}^{\otimes 2} \otimes \mathcal{H}_{\mathcal{N}_c} \otimes \mathcal{H}_{\mathcal{N}_w})$ definido por

$$\mathbf{W} |a\rangle |b\rangle |c\rangle |g\rangle = |a\rangle |b\rangle |c\rangle |(g + w(a,b,c)) \bmod S(\mathcal{N}_w)\rangle \quad . \tag{3.18}$$

A acção de $\mathbf{W}$, $\mathbf{W} |a\rangle |b\rangle |c\rangle |0\rangle = |a\rangle |b\rangle |c\rangle |w(a,b,c)\rangle$, ilustra-se na Figura 3.3.

O cálculo em paralelo dos dígitos soma parcial reduz-se a aplicar o seguinte produto de operadores unitários locais, que agem sobre conjuntos disjuntos de qudits,

$$\mathbf{L}_3 = \prod_{i=0}^{n-1} \mathbf{W}_i \equiv \mathbf{W}_{n-1}\mathbf{W}_{n-2} \cdots \mathbf{W}_1\mathbf{W}_0 \ , \tag{3.19}$$

onde $\mathbf{W}_i = \mathbf{W}[x_i, y_i, c_{i+1}, w_i]$, $i = 0, \ldots, n-1$.

O cálculo de cada dígito soma final, z_i, $i = 0, 1, \ldots, n-1$, é realizado pelo operador $\mathbf{Z} \in \mathcal{U}(\mathcal{H}_{\mathcal{N}_c} \otimes \mathcal{H}_{\mathcal{N}_w} \otimes \mathcal{H}_{\mathcal{N}})$ definido por

$$\mathbf{Z} |w\rangle |c\rangle |h\rangle = |w\rangle |c\rangle |(h + w + c) \bmod S(\mathcal{N})\rangle \quad . \tag{3.20}$$

Na figura 3.3 ilustra-se a acção de $\mathbf{Z}$, $Z |w\rangle |c\rangle |0\rangle = |w\rangle |c\rangle |w + c\rangle$.

Sejam $\mathbf{Z}_i = \mathbf{Z}[w_i, c_i, z_i]$, $i = 0, \ldots, n-1$. O cálculo em paralelo dos dígitos soma final é alcançado com a aplicação do operador unitário

$$\mathbf{L}_4 = \prod_{i=0}^{n-1} \mathbf{Z}_i \ . \tag{3.21}$$

Note-se que o dígito mais significativo do resultado, z_n, havido já sido calculado como um dígito de transporte.

De modo a reverter o estado dos qudits ancilares ao seu estado inicial, inverte-se a acção das portas $\mathbf{E}$, $\mathbf{C}$ e $\mathbf{W}$ na seguinte ordem:

$$\mathbf{L}_5 = \mathbf{W}_0^\dagger \mathbf{W}_1^\dagger \cdots \mathbf{W}_{n-2}^\dagger \mathbf{W}_{n-1}^\dagger \ , \tag{3.22}$$

$$\mathbf{L}_6 = \mathbf{C}_1^\dagger \mathbf{C}_2^\dagger \cdots \mathbf{C}_{n-2}^\dagger \mathbf{C}_{n-1}^\dagger \ , \tag{3.23}$$

$$\mathbf{L}_7 = \mathbf{E}_1^\dagger \mathbf{E}_2^\dagger \cdots \mathbf{E}_{n-2}^\dagger \mathbf{E}_{n-1}^\dagger \ . \tag{3.24}$$

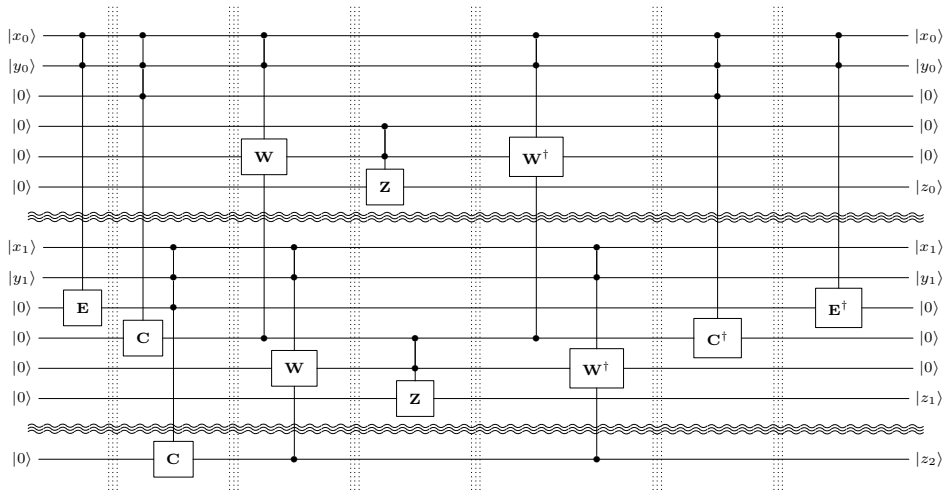


Figura 3.4: O circuito QLCPA para $n = 2$ qudits

Na figura 3.4 ilustra-se o circuito QLCPA para o caso $n = 2$. Todas as portas no interior de cada uma das 7 regiões verticais assinaladas podem ser aplicadas em simultâneo. O bloco delimitado pelas linhas horizontais onduladas demarca o lugar onde é possível inserir $n - 2$ blocos idênticos de modo a estender o circuito para lidar com o problema da adição de números com n dígitos. Independentemente do tamanho dos números, a profundidade do circuito QLCPA é constante (igual a 7).

Define-se em seguida o operador unitário correspondente ao circuito completo. Note-se que as portas **E** e **C** dependem do sistema de representação considerado.

Sejam $\mathcal{H}_{\text{work}} = \mathcal{H}_{\mathcal{N}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}}^{\otimes (n+1)}$ o espaço de Hilbert principal e $\mathcal{H}_{\text{ancilla}} = \mathcal{H}_2^{\otimes (n-1)} \otimes \mathcal{H}_{\mathcal{N}_c}^{\otimes n} \otimes \mathcal{H}_{\mathcal{N}_w}^{\otimes n}$ o espaço ancilar. O operador unitário $\mathbf{V} \in \mathcal{U}\left(\mathcal{H}_{\text{work}} \otimes \mathcal{H}_{\text{ancilla}}\right)$ definido por

$$\mathbf{V} = \mathbf{L}_7\mathbf{L}_6\mathbf{L}_5\mathbf{L}_4\mathbf{L}_3\mathbf{L}_2\mathbf{L}_1 \tag{3.25}$$

tem acção

$$\mathbf{V}(|x, y, 0\rangle \otimes |0\rangle) = \mathbf{U}(|x, y, 0\rangle) \otimes |0\rangle \quad , \tag{3.26}$$

onde $\mathbf{U}$ é o operador soma referido em (3.1).

3.1.3 O circuito QCFA no sistema $\mathrm{GSD}(3,3,4)$

Seja $\mathcal{N} = \mathrm{GSD}(3,3,4)$ o sistema simétrico convencional de dígitos com sinal, de redundância máxima, $\rho = 2$, em raiz $r = 4$. Como consequência do teorema 3.1, é possível definir um circuito QCFA para adição de dois números neste sistema.

Mostra-se que $\mathcal{N}_c = \mathrm{GSD}(1,1,2)$ e cada dígito de transporte é calculado com a função

$$c(x_i, y_i) = \begin{cases} -1 & \text{se } x_i + y_i \leq -3 \\ 0 & \text{se } -2 \leq x_i + y_i \leq 2 \\ 1 & \text{se } x_i + y_i \geq 3. \end{cases}$$

A partir da figura desta função, figura 3.5, constrói-se o circuito representado na figura 3.6, baseado em portas de Tofolli generalizadas, onde $\mathbf{X}$ denota o operador definido por $\mathbf{X}\,|a\rangle = |(a+1) \bmod S(\mathcal{N}_c)\rangle$ (veja-se a figura 3.7).

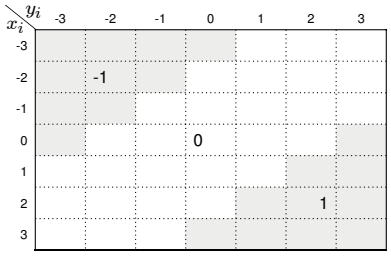


Figura 3.5: Cálculo dos dígitos de transporte no sistema $\mathrm{GSD}(3,3,4)$

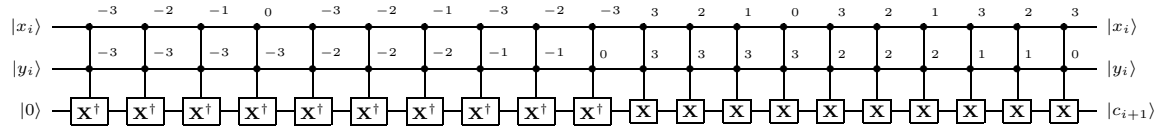


Figura 3.6: Implementação em série da porta $\mathbf{C}$

É possível reduzir substancialmente a profundidade da porta $\mathbf{C}$ recorrendo a portas de *limiar* e utilizando algum espaço ancilar. De facto, a profundidade do circuito ilustrado na figura 3.8, equivalente ao circuito na figura 3.6, é apenas[1] 5.

[1] Note-se que é possível implementar cada porta de *limiar* com um circuito quântico de profundidade 3.

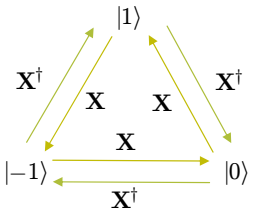


Figura 3.7: A acção do operador **X** no cálculo dos dígitos de transporte

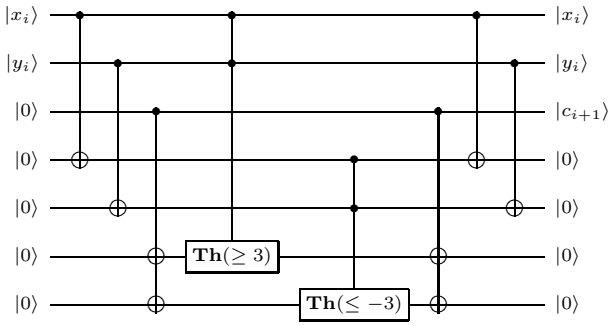


Figura 3.8: Implementação em paralelo da porta **C**

O cálculo de cada dígito soma parcial é realizado pela função representada na figura 3.9 e o circuito quântico correspondente obtém-se de forma análoga à do circuito para o cálculo dos dígitos de transporte.

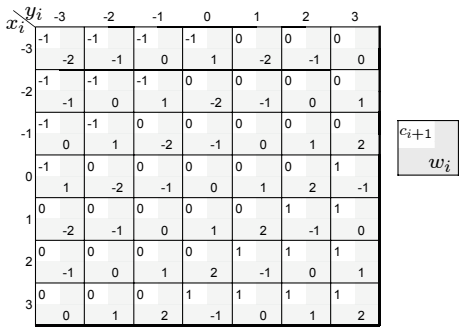


Figura 3.9: Cálculo das somas parciais no sistema GSD$(3, 3, 4)$

O cálculo de cada dígito soma final obtém-se com um circuito que implementa a versão reversível de um somador 2 para 1.

O somador LCPA no sistema $\mathrm{GSD}(0, 2, 2)$

O factor de redundância do sistema de representação em raiz 2 com guarda de transporte, $\mathcal{N} = \mathrm{GSD}(0, 2, 2)$, é $\rho = 2$. Neste sistema, as estimativas para os dígitos de transporte são dadas por

$$e_{i+1} = \begin{cases} 0 & \text{se } x_i + y_i < 2 \\ 1 & \text{se } x_i + y_i \geq 2 \end{cases} . \tag{3.27}$$

Os dígitos de transporte são calculados pela função

$$c_{i+1} = \begin{cases} 0 & x_i + y_i + e_i < 2 \\ 1 & \text{se } 2 \leq x_i + y_i + e_i < 4 \\ 2 & \text{se } x_i + y_i + e_i \geq 4 \end{cases} \tag{3.28}$$

Cada uma das portas quânticas básicas para o circuito LCPA são implementáveis de forma exacta usando um esquema sequencial de portas de Tofolli generalizadas, ou de forma aproximada, com uma profundidade muito menor, usando portas de *limiar*.

3.2 Adição de m inteiros

Considere-se a seguinte especificação para $\mathbf{Soma}_{\mathcal{N}}(m, n)$, o problema de calcular a soma de m números inteiros de tamanho n:

> Dados m números inteiros x_i, $i = 1, \ldots, m$, representados no sistema $\mathcal{N} = \mathrm{GSD}(\alpha, \beta, r)$ por sequências de n dígitos $x_{i,j} \in S(\mathcal{N})$, $j = 0, \ldots, n-1$, determine-se uma representação para o inteiro $\sum_{i=1}^{m} x_i$.

Reescreva-se $T = \sum_{i=0}^{m-1} x_i$ na forma $T = \sum_{j=0}^{n-1} s_j r^j$, onde $s_j = \sum_{i=0}^{m-1} x_{ij}$. Decomponha-se s_j num dígito de transporte c_{i+1} e numa soma temporária w_j, i.e, $s_j = rc_{j+1} + w_j$. Considerando $c_0 = 0$, obtém-se

$$T = \sum_{j=0}^{n-1} (rc_{j+1} + w_j) r^j = c_n r^n + \sum_{j=0}^{n-1} (w_j + c_j) r^j.$$

Finalmente, considerando $z_j = w_j + c_j$, $j = 0, \ldots, n-1$, obtém-se $T = c_n r^n + \sum_{j=0}^{n-1} z_j r^j$.

Daqui resulta o seguinte algoritmo sem Propagação de Dígitos de Transporte:

Algoritmo 3.3. Adição sem Propagação de Dígitos de Transporte (CFA) para a resolução do problema $\mathbf{Soma}_{\mathcal{N}}(m,n)$:

```
PARA j DESDE 0 ATÉ n-1
  calcular c[j+1] e w[j] usando s[j];
PARA j DESDE 0 ATÉ n-1
  calcular z[j] usando w[j] e c[j].
```

Lema 3.1. Considere-se um sistema de representação $\mathcal{N} = \mathrm{GSD}(\alpha, \beta, r)$ com coeficiente de redundância ρ. O algoritmo 3.3 é aplicável ao problema $\mathbf{Soma}_{\mathcal{N}}(m,n)$ se e só se existem inteiros λ e μ tais que $\lambda \geq (m-1)\rho^-$, $\mu \geq (m-1)\rho^+$ e $\rho \geq 1 + \frac{\lambda+\mu}{r-1}$.

Demonstração. Sejam $\lambda, \mu \geq 0$, inteiros tais que

$$\forall j,\ c_j \in [-\lambda \mathinner{..} \mu]\ . \tag{3.29}$$

Uma vez que $z_j \in S(\mathcal{N})$ e $w_j = z_j - c_j$, conclui-se que os dígitos de soma temporária devem satisfazer a condição

$$w_j \in [-\alpha + \lambda \mathinner{..} \beta - \mu]\ . \tag{3.30}$$

No algoritmo 3.3, para cada s_j, é necessário determinar um dígito de transporte c_{j+1} de modo que $w_j = s_j - rc_{j+1}$ satisfaça (3.30). Assim, cada dígito de transporte c_{j+1} deve verificar a condição

$$\frac{s_j - \beta + \mu}{r} \leq c_{j+1} \leq \frac{s_j + \alpha - \lambda}{r}\ . \tag{3.31}$$

Note-se que $s_j = \sum_{i=0}^{m-1} x_{ij} \in [-m\alpha \mathinner{..} m\beta]$. Sejam $a(s) = \left\lceil \frac{s-\beta+\mu}{r} \right\rceil$ e $b(s) = \left\lfloor \frac{s+\alpha-\lambda}{r} \right\rfloor$. Combinando as condições (3.29) e (3.31) conclui-se que o algoritmo 3.3 é aplicável ao problema $\mathbf{Soma}_{\mathcal{N}}(m,n)$ se e só se existem inteiros $\lambda, \mu \geq 0$ tais que

$$\forall s \in [-m\alpha \mathinner{..} m\beta]\,,\ [a(s) \mathinner{..} b(s)] \cap [-\lambda \mathinner{..} \mu] \neq \emptyset\ . \tag{3.32}$$

A intersecção em (3.32) é não vazia se e só se $a(s) \leq b(s)$,$-\lambda \leq b(s)$ e $\mu \geq a(s)$.

Sejam ξ e δ respectivamente o quociente e o resto da divisão inteira de $s - \lambda + \alpha$ por r, i.e, $s - \lambda + \alpha = \xi r + \delta$, com $0 \leq \delta \leq r-1$. A condição $a(s) \leq b(s)$ é equivalente a $\delta \leq \alpha + \beta - (\lambda + \mu)$. Mostra-se ainda que o resto $\delta = r - 1$ é atingível, isto é, existe $s \in [-m\alpha \mathinner{..} m\beta]$ tal que $s - \lambda + \alpha = \xi r + r - 1$. Assim $a(s) \leq b(s)$ se e só se $\rho \geq 1 + \frac{\lambda+\mu}{r-1}$.

Finalmente, as condições $-\lambda \leq b(s)$ e $\mu \geq a(s)$ são, respectivamente, equivalentes a $\lambda \geq (m-1)\rho^-$ e $\mu \geq (m-1)\rho^+$. □

Teorema 3.2. Seja ρ o coeficiente de redundância de um sistema de representação $\mathcal{N} = \mathrm{GSD}(\alpha, \beta, r)$. O algoritmo 3.3 é aplicável ao problema $\mathbf{Soma}_{\mathcal{N}}(m, n)$ se e só se

$$\rho \geq 1 + \frac{\lceil (m-1)\rho^- \rceil + \lceil (m-1)\rho^+ \rceil}{r-1} \tag{3.33}$$

Demonstração. Pelo lema anterior, o conjunto mínimo de dígitos de transporte, $[-\lambda \,..\, \mu]$, satisfaz $\lambda = \lceil (m-1)\rho^- \rceil$ e $\mu = \lceil (m-1)\rho^+ \rceil$. □

Observação 3.2. As seguintes observações são consequência do teorema anterior:

1. O teorema 3.1 corresponde ao caso $m = 2$ no teorema anterior.

2. Para $m > r - 1$ não é possível aplicar o algoritmo 3.3.

3. Após uma análise exaustiva e ao contrário do caso $m = 2$, não parece ser possível obter um conjunto de condições simples sobre os parâmetros α, β e r que sejam equivalentes a 3.33. Assim para cada sistema de representação considerado é necessário verificar à priori aquela condição.

No contexto da Computação Clássica em Redes Neuronais, Cotofana e Vassiliadis [12] demonstram a possibilidade de construir um circuito para o problema $\mathbf{Soma}_{\mathcal{N}}(m, n)$ no caso dos sistemas simétricos ($\alpha = \beta$) de raiz $r = 2$. Mais precisamente para $m = \mathcal{O}(n)$ obtêm um circuito de tamanho $\mathcal{O}\left(n^3\right)$ e profundidade 2. A ideia subjacente ao algoritmo consiste em interpretar cada parcela de n dígitos em raiz r como um número num sistema de representação de raiz r^k para $k = \log m$. Usando um esquema análogo, é possível obter um circuito quântico com características semelhantes, embora com profundidade um pouco maior (mas constante), que implementa o algoritmo 3.3, uma vez que cada porta de *limiar* quântica é aproximável em profundidade constante recorrendo a portas de *fanout*.

Simulação de Algoritmos Quânticos $\langle 4|$

"by golly it's a wonderful problem
because it doesn't look so easy"
Richard Feynman

Nas mais diversas áreas científicas é comum verificar-se um grau superior de desenvolvimento teórico relativamente às aplicações práticas. A área da Computação Quântica não constitui excepção já que os enormes progressos ao nível teórico não têm tido paralelo ao nível tecnológico. E não será por falta de investigação, ou investimento, mas pela extrema dificuldade dos problemas práticos que se colocam. Apesar das diversas propostas avançadas, a realização física de um computador quântico, o desenvolvimento de hardware quântico e a integração de componentes quânticas são processos ainda na sua infância. Tem sido veiculada a necessidade de aguardar várias décadas para que a tecnologia quântica seja disponibilizada em larga escala. Daí, que o problema de simular processos quânticos em computadores clássicos seja pertinente e actual.

Em 1982, Feynman [24] observou que a simulação da evolução de sistemas quânticos era um processo inerentemente complexo. Por um lado, porque é necessário representar os possíveis estados do sistema e cada estado de um sistema quântico fechado composto por n d-qudits é um vector de norma um, pertencente a um espaço de Hilbert de dimensão d^n. Também, porque a discretização da evolução temporal de um sistema quântico fechado consiste na acção sequencial de operadores unitários sobre o estado inicial do sistema. Finalmente, porque o processo de observação do estado final requer técnicas de simulação de amostragem sobre distribuições de probabilidade com suporte no conjunto dos estados base do sistema (conjunto

esse de cardinal d^n).

Uma forma directa de atacar o problema da simulação de algoritmos quânticos, aqui designada abordagem vectorial, consiste em representar os estados por vectores de componentes complexas e simular a evolução com produtos matriciais. Tanto quanto foi possível averiguar, a generalidade dos simuladores existentes seguem esta abordagem, desde simples aplicações [14, 20] até um cluster de dezenas de processadores que permite simulações da evolução de sistemas quânticos até um máximo de 30 qubits [47].

Na origem do desenvolvimento de uma forma alternativa de abordar este problema, aqui designada abordagem simbólica, salienta-se a seguinte observação.

> Existe uma relação forte entre a complexidade da simulação e o entrelaçamento dos sucessivos estados na evolução de um sistema quântico.

De facto, espera-se que um algoritmo quântico admita uma simulação eficiente sempre que, ao longo do processo, ocorra somente entrelaçamento local entre um número pequeno de qudits.

Neste capítulo descrevem-se, em traços largos, as principais características do *Simulador Simbólico de Computação Quântica*, sqcs, desenvolvido para o sistema de computação algébrica *Mathematica* [54]. Os objectivos chave definidos no início do desenvolvimento do simulador simbólico são: identificar, controlar e compreender o inerente crescimento exponencial dos recursos espaciais e temporais presentes no decorrer das simulações.

Por forma a ilustrar esta abordagem, considerou-se a simulação de um dos algoritmos que marcam a história da computação quântica: o algoritmo de Grover. Assim, na parte final deste capítulo, apresentam-se e discutem-se os tempos obtidos nas simulações.

4.1 Descrição do simulador

Ao iniciar o desenvolvimento de um simulador de Computação Quântica sobre um sistema computacional algébrico como o *Mathematica*, a primeira observação a ter em conta é que o essencial na representação de objectos é a sua descrição e não o seu conteúdo. As aplicações existentes, mesmo as desenvolvidas para o *Mathematica*, parecem não considerar este facto.

Por exemplo, é preferível representar qualquer estado base de um d-qudit como um objecto simbólico, a utilizar uma lista de d números complexos (mesmo que na forma de uma tabela compactada). Quaisquer operações subsequentes sobre estes objectos devem ser implementadas de uma forma estritamente simbólica. Exemplo disso é a simulação da acção de um qualquer operador unitário sobre um estado por intermédio de um conjunto de regras algébricas previamente especificadas.

Apresentam-se em seguida os objectos principais e operações básicas no SQCS. Salienta-se que a maioria dos objectos e operações possuem notações externas, convenientes para utilização no 'frontend', associadas às representações internas utilizadas pelo 'kernel' do *Mathematica*.

4.1.1 Kets

Recorde-se que um *qudit* é um sistema quântico cujo estado é representável por um vector de norma um pertencente a um espaço de Hilbert de dimensão d. No que se segue, assume-se que o espaço de Hilbert subjacente é sempre $\mathcal{H}_d = \mathbb{C}^d$ e faz-se uso da notação de Dirac para identificar a base computacional canónica de $\mathcal{H}_d$ com o conjunto $\{|k\rangle, k \in \mathbb{Z}_d\}$.

Assim o estado geral de um qudit é $|\psi\rangle = \sum_{k\in\mathbb{Z}_d} a_k |k\rangle$, em que $a_k \in \mathbb{C}$, para $k \in \mathbb{Z}_d$ e $\sum_{k\in\mathbb{Z}_d} |a_k|^2 = 1$. O caso $d = 2$ corresponde à definição usual do estado de um *qubit*, $|\psi\rangle = a|0\rangle + b|1\rangle$ em que $|a|^2 + |b|^2 = 1$, $a, b \in \mathbb{C}$.

No SQCS cada estado base de um qudit é representado por um objecto simbólico denominado `ket` . Algumas das formas textuais reconhecidas são:

- `ket[0]`, `ket[1]` — os estados base de um qubit.
- `ket[i_Integer,n_Integer]` — o i-ésimo estado base de um n-qudit.

O comando `<Esc>ket<Esc>` permite introduzir de forma simples objectos `ket` no simulador. Na figura 4.1 ilustram-se alguns exemplos e propriedades.

4.1.2 Bras

Recorde-se que o conjunto dos funcionais lineares num espaço de Hilbert $\mathcal{H}$ é também um espaço de Hilbert, o espaço dual de $\mathcal{H}$, denotado por $\mathcal{H}^\dagger$. De acordo com o teorema de Riesz,

```
<< SQCS`
{ket[0], ket[1], ket[0, 3], ket[1, 3], ket[2, 3]}
```

$$\{|0\rangle, |1\rangle, |0_3\rangle, |1_3\rangle, |2_3\rangle\}$$

```
α |ψ⟩ + α |ϕ⟩ // Simplify
```

$$\alpha\,(|\phi\rangle + |\psi\rangle)$$

```
α |ϕ⟩ + β |ϕ⟩ // Simplify
```

$$(\alpha + \beta)\,|\phi\rangle$$

```
|ϕ⟩ - |ϕ⟩
```

$$0$$

```
<< SQCS`
|ψ0⟩ = 1 / Sqrt[2] |0⟩ + I / Sqrt[2] |1⟩
```

$$\frac{|0\rangle}{\sqrt{2}} + \frac{i\,|1\rangle}{\sqrt{2}}$$

```
|ψ1⟩ = I |ψ0⟩ + 1 / Sqrt[2] |1⟩
```

$$\frac{|1\rangle}{\sqrt{2}} + i\left(\frac{|0\rangle}{\sqrt{2}} + \frac{i\,|1\rangle}{\sqrt{2}}\right)$$

```
|ψ1⟩ // Simplify
```

$$\frac{i\,|0\rangle}{\sqrt{2}}$$

Figura 4.1: Algumas regras algébricas e exemplos de objectos `ket`

```
<< SQCS`
{bra[0], bra[1], bra[0, 3], bra[1, 3], bra[2, 3]}
```

$$\{\langle 0|, \langle 1|, \langle 0_3|, \langle 1_3|, \langle 2_3|\}$$

```
(α |ψ⟩ + β |ϕ⟩)†
```

$$\langle\psi|\,\alpha^* + \langle\phi|\,\beta^*$$

```
<< SQCS`
|ψ0⟩ = 1 / Sqrt[2] |0⟩ + I / Sqrt[2] |1⟩
```

$$\frac{|0\rangle}{\sqrt{2}} + \frac{i\,|1\rangle}{\sqrt{2}}$$

```
|ψ0⟩†
```

$$\frac{\langle 0|}{\sqrt{2}} - \frac{i\,\langle 1|}{\sqrt{2}}$$

Figura 4.2: Algumas propriedades de objectos `bra`

o produto interno em $\mathcal{H}$ induz uma correspondência biunívoca entre os elementos de $\mathcal{H}$ e os elementos de $\mathcal{H}^\dagger$. Na notação de Dirac, o dual do *ket* $|\psi\rangle \in \mathcal{H}$ é o *bra* $\langle\psi| = |\psi\rangle^\dagger \in \mathcal{H}^\dagger$. No `SQCS` o dual de um objecto `ket` é um objecto `bra`. Algumas das formas admissíveis para objectos `bra` são:

- `bra[0]`, `bra[1]` — os duais dos estados base de um qubit.
- `bra[i_Integer,n_Integer]` — o dual do i-ésimo estado base de um n-qudit.

O comando `<Esc>bra<Esc>` permite introduzir objectos `bra` no simulador. A figura 4.2 ilustra algumas exemplos e propriedades destes objectos bem como da função `dagger`.

```
<< SQCS`
{⟨0 | 1⟩, ⟨1 | 1⟩, ⟨1₃ | 2₃⟩}
{0, 1, 0}
{⟨0 | · | 1⟩, ⟨1 | · | 1⟩, ⟨1₃ | · | 2₃⟩}
{0, 1, 0}
```

```
<< SQCS`
(α ⟨ψ | + β ⟨ϕ |) · | η⟩ //. expandInnerProduct
⟨ψ | η⟩ α* + ⟨ϕ | η⟩ β*
⟨η | · (α | ϕ⟩ + β | ψ⟩) //. expandInnerProduct
α ⟨η | ϕ⟩ + β ⟨η | ψ⟩
```

Figura 4.3: Algumas regras algébricas do produto interno de kets

4.1.3 Produto Interno e BraKets

Seja $\langle\psi| \in \mathcal{H}^\dagger$. Recorde-se que a acção deste funcional linear em $\mathcal{H}$ sobre um *ket*, $|\phi\rangle \in \mathcal{H}$, tem como resultado um número complexo, $\langle\psi|\,(|\phi\rangle)$, denotado simplesmente por um *braket*, $\langle\psi|\phi\rangle$.

O comando `<Esc>braket<Esc>` permite a introdução de objectos `braKet` no simulador. As formas textuais `braKet` reconhecidas são `braKet[{x_},{y_}]`, onde `x_` e `y_` são sequências definidas de modo a que `bra[x_]` e `ket[y_]` correspondam, respectivamente, a formas textuais `bra` e `ket` admissíveis.

Os objectos `braKet` possuem uma interpretação alternativa. De facto, no espaço de Hilbert $\mathcal{H}$ define-se um produto interno de estados. (Convenciona-se que o produto interno é linear conjugado no primeiro argumento e linear no segundo.) Se se denotar o produto interno de $|\psi\rangle$ e $|\phi\rangle$ por $\langle\psi| \cdot |\phi\rangle$ então $\langle\psi| \cdot |\phi\rangle = \langle\psi|\phi\rangle = \langle\psi|\,(|\phi\rangle)$.

Para definir formas textuais de produtos internos é possível utilizar tanto o operador infix `**` como a função `inner[_,_]`. O comando `<Esc>.<Esc>` permite também introduzir a forma infix da operação produto interno no simulador. A figura 4.3 contém alguns exemplos.

4.1.4 Produto de Kronecker

Recorde-se que o espaço de Hilbert subjacente a um sistema quântico composto é o produto tensorial dos espaços de Hilbert subjacentes aos subsistemas. Assim, o estado de um sistema quântico constituído por n d-qudits é um vector de norma um em $\mathcal{H}_d{}^{\otimes n}$. A base computacional deste espaço é constituída por d^n estados base $|x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle$, em que $x_j \in \mathbb{Z}_d$, $j = 0, 1, \ldots, n-1$.

```
<< SQCS`
|φ⟩⊗(|ψ⟩⊗|η⟩) === (|φ⟩⊗|ψ⟩)⊗|η⟩
True
(α|φ⟩)⊗|ψ⟩
α|φ⟩⊗|ψ⟩
|φ⟩⊗(α|ψ⟩)
α|φ⟩⊗|ψ⟩
```

```
<< SQCS`
(α|φ⟩+β|ψ⟩)⊗|η⟩ //. expandKron
α|φ⟩⊗|η⟩+β|ψ⟩⊗|η⟩
|η⟩⊗(α|φ⟩+β|ψ⟩) //. expandKron
α|η⟩⊗|φ⟩+β|η⟩⊗|ψ⟩
(|0⟩+|1⟩)^⊗2 /. expandPow //. expandKron
|0⟩⊗|0⟩+|0⟩⊗|1⟩+|1⟩⊗|0⟩+|1⟩⊗|1⟩
```

Figura 4.4: Algumas propriedades algébricas do produto tensorial

Cada um dos estados base associa-se de forma natural a um inteiro representado por uma sequência de n dígitos em base d, donde são equivalentes as seguintes notações:

$$|x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle \equiv |x_{n-1} \cdots x_1 x_0\rangle \equiv \left| \sum_{j=0}^{n-1} x_j d^j \right\rangle .$$

O produto tensorial, também conhecido por produto de Kronecker, é associativo, não comutativo e distributivo relativamente a combinações lineares. No SQCS definem-se produtos tensoriais utilizando quer a forma infix do operador $\otimes$, com o comando `<Esc>c*<Esc>`, quer a função `kron[_,__]`. A figura 4.4 inclui alguns exemplos.

4.1.5 Operadores

No SQCS os operadores lineares são representados por objectos `op[name_,n_,f_]`, em que `name` é o nome do operador, `n` é o número de qudits sobre os quais a acção do operador é definida, e `f` é uma função que define a acção do operador sobre os kets base.

Existem vários operadores disponíveis no simulador, como por exemplo o operador identidade I_n, em que o índice n indica o número de qudits em que o operador actua[1]. Outros exemplos são:

[1] Diverge-se aqui da notação usual em que o índice designa a dimensão do espaço de Hilbert subjacente.

```
<< SQCS`
numericOff
H · | 0⟩
(| 0⟩ + | 1⟩)/√2
H · | 1⟩
(| 0⟩ - | 1⟩)/√2
```

```
<< SQCS`
numericOff
H · (| 0⟩ + | 1⟩)/√2 //. expandLinearInside // Simplify
| 0⟩
H · H
I₁
```

Figura 4.5: A acção do operador de Hadamard

Operador de Hadamard

Um operador fundamental em Computação Quântica, que permite criar sobreposições uniformes de estados base, é o operador de Hadamard, $\mathbf{H}$. A acção deste operador sobre um qubit é dada por

$$\mathbf{H}\,|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^i\,|1\rangle\right),\ i = 0, 1.$$

Na figura 4.5 ilustra-se o facto de que H ser inverso dele próprio. É possível utilizar o comando `<Esc>opH<Esc>` para introduzir este operador no simulador.

Operador de Walsh-Hadamard

Recorde-se que $\mathrm{H}^{\otimes n}$ denota o operador de Walsh-Hadamard em n qubits. A acção deste operador em cada estado base $|i\rangle$, $i = 0, \ldots, 2^n - 1$, é

$$\mathbf{H}^{\otimes n}\,|i\rangle = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{i\cdot j}\,|j\rangle\ , \tag{4.1}$$

em que $i \cdot j$ denota o produto interno módulo 2 das representações binárias de i e j. Na figura 4.6 ilustram-se algumas propriedades do operador de Walsh-Hadamard. A implementação deste operador baseia-se no conceito geral de potências tensoriais de objectos, conceito totalmente suportado no `SQCS`. Note-se que a simulação da acção deste operador sobre um estado é internamente um processo estritamente simbólico e eficiente em termos dos recursos de memória utilizados. Veja-se o apêndice B para uma descrição da decomposição do operador de Walsh-Hadamard e consequente justificação da afirmação anterior.

```
<< SQCS`
numericOff;
H^⊗4 · |0⟩^⊗4
(1/4) (|0⟩ + |1⟩)^⊗4
H^⊗3 · |0⟩⊗|1⟩⊗|0⟩
((|0⟩ + |1⟩)⊗(|0⟩ - |1⟩)⊗(|0⟩ + |1⟩))/(2√2)
```

```
<< SQCS`
numericOff;
H^⊗2 · |0⟩⊗|1⟩ /. expandKron
(1/2) (|0⟩⊗|0⟩ - |0⟩⊗|1⟩ + |1⟩⊗|0⟩ - |1⟩⊗|1⟩)
H^⊗5 · H^⊗5
I_5
```

Figura 4.6: A acção do operador de Walsh-Hadamard

```
<< SQCS`
(|ψ⟩ · ⟨ϕ|) · |η⟩
⟨ϕ|η⟩ |ψ⟩
(|0⟩ · ⟨1|)^⊗4 · (|0⟩⊗|0⟩⊗|1⟩⊗|1⟩)
0
(|0⟩ · ⟨1|)^⊗4 · (|1⟩⊗|1⟩⊗|1⟩⊗|1⟩)
|0⟩⊗|0⟩⊗|0⟩⊗|0⟩
```

```
<< SQCS`
(Σ_{i=0}^{3} |i_4⟩ · ⟨i_4|) · |0_4⟩ //. expandLinearOutside
|0_4⟩
```

Figura 4.7: A acção do operador Produto Externo

Operador Produto Externo

Considere-se o espaço de Hilbert $\mathcal{H} = {\mathcal{H}_d}^{\otimes n}$ e sejam $|i\rangle, |j\rangle \in \mathcal{H}$ dois estado base. A acção do operador linear Produto Externo, $|i\rangle\langle j|$, sobre estados base $|k\rangle$, $k = 0, \ldots, d^n - 1$, define-se por

$$(|i\rangle\langle j|)\,|k\rangle = \langle j|k\rangle\,|i\rangle \ . \tag{4.2}$$

Uma propriedade útil que envolve operadores Produto Externo é a relação de totalidade $\sum_{i=0}^{d^n-1} |i\rangle\langle i| = \mathrm{I}_n$. Na figura 4.7 exibem-se algumas propriedades deste operador e no apêndice B mostra-se que, sob certas condições, admite uma implementação eficiente e puramente simbólica.

4.1.6 Comentário

As características descritas nas secções anteriores correspondem a uma versão inicial do simulador(SQCS v0.x) orientada para a simulação de vários algoritmos quânticos em sistemas não híbridos de qubits ou qudits.

Com o início do desenvolvimento dos algoritmos quânticos para aritmética em sistemas generalizados de dígitos redundantes (capítulo 3) sentiu-se a necessidade de expandir o SQCS no sentido de este permitir a representação de estados e operadores nesses sistemas bem como testar aqueles algoritmos. Iniciou-se assim o desenvolvimento de uma nova versão (SQCS v1.x) a qual possui diferenças significativas comparativamente com a versão SQCS v0.x. Destacam-se os seguintes aspectos:

- Cada *ket* é um objecto simbólico `ket`[`x_`, `S_GSD`] onde `x` é um dígito de um sistema generalizado `S`. Cada sistema generalizado é um objecto da forma `GSD`[α`_`, β`_`, `r_`].

- Por forma a caracterizar os operadores lineares nestes sistemas considerou-se um novo objecto `space`[`n_`, `S_GSD`] o qual representa o espaço de Hilbert associado a um registo de `n` qudits de tal forma que os possíveis estados de cada um dos qudits são dados por kets num sistema generalizado `S`. Desenvolveu-se a especificação das regras algébricas associadas a objectos `space`, em particular as regras relativas ao produto tensorial de espaços de Hilbert.

- Cada operador linear é, nesta versão, um objecto da forma `op`[`name_`, `sp_`] onde `name` é o nome do operador e `sp` representa o espaço de Hilbert subjacente ao operador (um objecto `space` ou um produto tensorial de objectos `space`). A especificação propriamente dita da acção do operador em objectos `ket` foi transportada para fora da definição do operador. Desta forma, a menos que exista uma especificação adicional, cada operador tem por defeito um comportamento inerte. Esta abordagem permite controlar de forma mais precisa o momento em que ocorre a expansão de uma qualquer expressão associada à acção de um operador sobre um estado.

- Iniciou-se ainda o desenvolvimento de uma especificação do conceito de registo quântico. O objectivo a atingir numa versão futura do SQCS é que cada *ket* seja um objecto local

a um registo, o que permitirá especificar de forma precisa o conceito de acção local de um operador sobre um estado.

4.2 O algoritmo de Grover

Considere-se o problema de pesquisa numa base de dados não ordenada. Seja $N = 2^n$ o número de elementos de uma base de dados indexados pelos inteiros $0, 1, \ldots, N-1$. Seja $x^\star$ o índice do único elemento que possui uma determinada propriedade. O problema consiste em determinar $x^\star$.

No contexto da Computação Clássica, demonstra-se que a resolução deste problema por qualquer algoritmo (determinista ou probabilístico) requer, em média, $N/2$ acessos à base de dados. No entanto, em 1996, Lov Grover [27] publicou um algoritmo quântico que usa apenas $\mathcal{O}\left(\sqrt{N}\right)$ consultas à base de dados.

Segue-se uma descrição sintética do algoritmo de Grover. Para uma análise mais completa e generalizações consulte-se, por exemplo, Biham et al. [7].

Assume-se a existência de uma função oráculo definida por

$$f(x) = \begin{cases} 1 & \text{se } x = x^\star \\ 0 & \text{caso contrário.} \end{cases} \tag{4.3}$$

No contexto da Computação Quântica, o oráculo corresponde a um operador unitário $\mathbf{U}_f$ definido por $|x\rangle \otimes |y\rangle \;\mapsto\; |x\rangle \otimes |f(x) \oplus y\rangle$, em que $\oplus$ denota a adição módulo 2.

A acção do oráculo $\mathbf{U}_f$ é equivalente à acção do operador unitário $\mathbf{I}_{|x^\star\rangle}$ definido por

$$\mathbf{I}_{|x^\star\rangle} |x\rangle = \begin{cases} -|x^\star\rangle & \text{se } x = x^\star \\ |x\rangle & \text{caso contrário.} \end{cases} \tag{4.4}$$

De facto, $\mathbf{U}_f \left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\mathbf{I}_{|x^\star\rangle} |x\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Note-se ainda que é possível escrever $\mathbf{I}_{|x^\star\rangle}$ na forma $\mathbf{I}_{|x^\star\rangle} = \mathbf{I} - 2\,|x^\star\rangle\langle x^\star|$. O algoritmo de Grover faz ainda uso do operador $\mathbf{I}_{|0\rangle}$ definido por $\mathbf{I}_{|0\rangle} = \mathbf{I} - 2\,|0\rangle\langle 0|$.

O algoritmo é aplicado a um sistema quântico de n qubits, inicialmente no estado $|0\rangle$. O primeiro passo consiste em criar uma sobreposição uniforme dos possíveis resultados, pela

aplicação do operador de Walsh-Hadamard. Em seguida o estado do sistema é "rodado" sucessivamente até se aproximar do estado $|x^\star\rangle$. Cada uma das rotações resulta da acção do operador de Grover

$$\mathbf{Q} = -\,\mathbf{H}^{\otimes n}\,\mathbf{I}_{|0\rangle}\,\mathbf{H}^{\otimes n}\,\mathbf{I}_{|x^\star\rangle}\ . \tag{4.5}$$

Algoritmo 4.1 (Grover, 1996)**.**

- Inicializar o estado do sistema: $|\psi_0\rangle = |0\rangle^{\otimes n}$;
- Aplicar o operador de Walsh-Hadamard: $|\psi_1\rangle = \mathbf{H}^{\otimes n}\,|\psi_0\rangle$;
- Para i desde 1 até $k \approx \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ calcular $|\psi_{i+1}\rangle = \mathbf{Q}\,|\psi_i\rangle$;
- Observar $|\psi_{k+1}\rangle$ relativamente à base computacional $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$.

4.3 Simulação do algoritmo de Grover

Realizaram-se simulações do Algoritmo de Grover no sqcs em dois cenários distintos. No cenário I – Base de Dados Quântica – assumiu-se a existência de uma base de dados quântica bem como de um esquema eficiente de endereçamento. No cenário II – Base de Dados Clássica – utilizaram-se bases de dados clássicas e considerou-se o custo das consultas ao oráculo.

Nos dois cenários, a questão da observação do estado final do sistema foi ignorada de modo a evitar o problema de construir, a partir do estado final, amostras sobre uma distribuição de probabilidade sobre um número exponencial de valores.

Realizaram-se simulações com instâncias de tamanho compreendido entre 2^2 e 2^{32}. Os meios informáticos possuiam as seguintes especificações: Pentium IV, 3.0 GHz, 1 GB de RAM.

4.3.1 Simulações no cenário I – Bases de Dados Quânticas

Neste caso assumiu-se que o oráculo corresponde ao operador $\mathbf{I}_{|x^\star\rangle} = \mathbf{I} - 2\,|x^\star\rangle\langle x^\star|$. O índice $x^\star$ foi gerado de forma aleatória no conjunto $\{0, \ldots, 2^n - 1\}$ e nas simulações não se utilizaram de facto quaisquer bases de dados. Este esquema parece ser adequado quando o objectivo é testar o comportamento e correcção do algoritmo de Grover.

```
n = 30;
k = 2^n;
pos = Random[Integer, {0, k - 1}]; Print["POSITION= ", pos]


numIt = Round[Pi / (4 * ArcSin[1 / Sqrt[k]]) - 1 / 2];
Print["Number of Iterations= ", numIt];

posBin = IntegerDigits[pos, 2, n];
Ω = I_n - 2 * kron @@ ( | #1_GSD[0,1,2] ⟩⟨ #1_GSD[0,1,2] | &) /@ posBin

Grover = H^⊗n · (2 ( | 0 ⟩⟨ 0 | )^⊗n - I_n) · H^⊗n · Ω

| ψ_0 ⟩ = | 0 ⟩^⊗n

| ψ_1 ⟩ = H^⊗n · | ψ_0 ⟩

nestedApply[Grover, | ψ_1 ⟩, numIt] // Timing
```

Figura 4.8: Parte principal do programa em *Mathematica* para as simulações no cenário I

Na figura 4.8 lista-se o código do programa principal em *Mathematica* que, de forma resumida, consiste nos seguintes passos:

- Inicializar o tamanho da instância a simular: $k = 2^n$;
- Gerar aleatoriamente o índice, *pos*, do elemento alvo na base de dados;
- Definir o oráculo: Oracle $= \mathbf{I} - 2\,|pos\rangle\langle pos|$;
- Definir o operador de Grover por Grover $= \mathbf{H}^{\otimes n} \cdot (2(|0\rangle\langle 0|)^{\otimes n} - \mathbf{I}) \cdot \mathbf{H}^{\otimes n} \cdot$Oracle;
- Inicializar o estado do sistema de n qubits: $|\Psi_0\rangle = |0\rangle$;
- Aplicar o operador de Walsh-Hadamard a $|\Psi_0\rangle$: $|\Psi_1\rangle = \mathbf{H}^{\otimes n} \cdot |\Psi_0\rangle$;
- Iterar o operador de Grover `numIt` $= \lfloor \frac{\pi}{4 \arcsin(1/\sqrt{2^n})} \rfloor$ vezes.

A simulação da acção do operador de Grover consiste numa implementação eficiente da seguinte acção sequencial: Oracle, seguido de $\mathbf{H}^{\otimes n}$, seguido de $\mathbf{I}_{|0\rangle}$ e por último $\mathbf{H}^{\otimes n}$. O processo interno de cálculo baseia-se em regras de transformação. Por exemplo `expandLinearInside` – regras que definem a linearidade dos operadores, ou `expandLinearOutside` – propriedades distributivas dos operadores.

Resultados das simulações

No cenário I conduziram-se simulações para sistemas com $n \in \{2, \ldots, 32\}$ qubits (pesquisa numa base de dados de tamanho $N = 2^n$). Foi possível simular o algoritmo de Grover em sistemas com $n = 30$ qubits em menos de 5 minutos.

Como esperado, os tempos obtidos, ilustrados na figura 4.9, seguem uma curva exponencial quando medidos em termos do número de qubits enquanto que em termos do tamanho da base de dados seguem a curva da raiz-quadrada.

4.3.2 Simulações no cenário II – Bases de Dados Clássicas

Neste cenário gera-se inicialmente um base de dados clássica e define-se em seguida o operador oráculo por $\text{Oracle} \cdot |x\rangle = (-1)^{f(x)} |x\rangle$ onde $f(x)$ é a função oráculo (4.3).

Dado que não foi possível encontrar qualquer decomposição útil deste operador na forma de um produto tensorial de n operadores, foi necessário expandir completamente certos estados intermédios no decorrer da aplicação do operador de Grover.

O código do programa principal em *Mathematica* utilizado nas simulações encontra-se figura 4.10. De forma resumida, consiste em:

- Inicializar o tamanho da instância a simular $k = 2^n$;
- Gerar aleatoriamente o índice do elemento alvo na base de dados;
- Inicializar a base de dados de tamanho k;
- Definir o operador oráculo;
- Definir o operador de Grover: $\text{Grover} = \mathbf{H}^{\otimes n} \cdot (2(|0\rangle \langle 0|)^{\otimes n} - \mathbf{I}) \cdot \mathbf{H}^{\otimes n} \cdot \text{Oracle}$;
- Inicializar o estado do sistema: $|\Psi_0\rangle$ to $|0\rangle$;
- Aplicar o operador de Walsh-Hadamard: $|\Psi_0\rangle$, $|\Psi_1\rangle = \mathbf{H}^{\otimes n} \cdot |\Psi_0\rangle$;
- Iterar o operador de Grover $\texttt{numIt} = \lfloor \frac{\pi}{4 \arcsin(1/\sqrt{2^n})} \rfloor$ vezes.

Resultados das simulações

No cenário II conduziram-se simulações para sistemas com $n \in \{4, 5, \ldots, 16\}$ qubits (pesquisa numa base dados de tamanho $N = 2^n$).

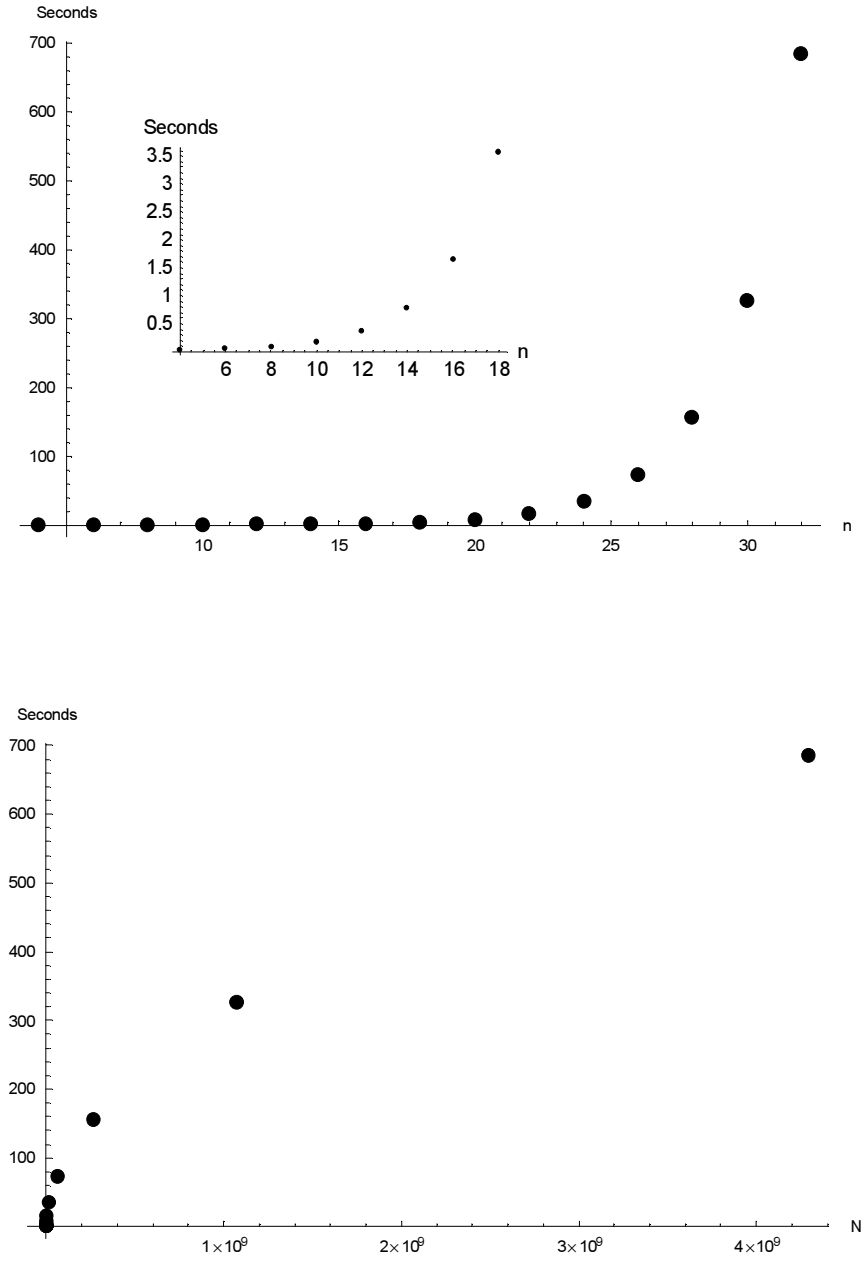


Figura 4.9: Tempos das simulações do algoritmo de Grover para uma base de dados quântica em função do número de qubits (n) e do tamanho da base de dados (N)

```
n = 5;
k = 2^n;
t = Table[0, {i, 0, k - 1}];
pos = Random[Integer, {0, k - 1}]; Print["POS=", pos]
t[[pos + 1]] = 1;
f[i_] := t[[i + 1]];

numIt = Round[Pi / (4 * ArcSin[1 / Sqrt[k]]) - 1 / 2];
Print["Number of Iterations = ", numIt];

Ω = oracle[f, n]

Grover = H^⊗n · (2 ( | 0 ⟩⟨ 0 | )^⊗n - I_n) · H^⊗n · Ω

| ψ0⟩ = | 0⟩^⊗n

| ψ1⟩ = H^⊗n · | ψ0⟩

nestedApply[Grover, | ψ1⟩, numIt] // Timing
```

Figura 4.10: Parte principal do programa em *Mathematica* para as simulações no cenário II

A figura 4.11 apresenta os tempos obtidos em função do número de qubits bem como em função do tamanho da base de dados. Os gráficos seguem a curva exponencial e explicam-se pela inerente ineficiência de simular as consultas ao oráculo.

4.4 Conclusões

As simulações do algoritmo de Grover realizadas, permitiram isolar e identificar a origem da complexidade do mesmo. De facto a complexidade dessas simulações não resulta do algoritmo em si mesmo, mas das consultas ao oráculo. Por outras palavras é ineficiente simular o acesso quântico a uma base de dados.

À posteriori, constatou-se que a estrutura da expressão simbólica associada ao estado final de cada simulação permitia identificar facilmente o resultado (índice) mais provável bem como a respectiva probabilidade. Assim, para este algoritmo, o problema da simulação da medição final do estado do sistema não se coloca. Se esta é uma característica exclusiva deste algoritmo ou uma propriedade mais geral do SQCS é uma questão que fica em aberto.

Em jeito de conclusão, conjectura-se que os sistemas de Computação Algébrica, como o *Mathematica*, são ambientes propícios para a implementação de simuladores na área da

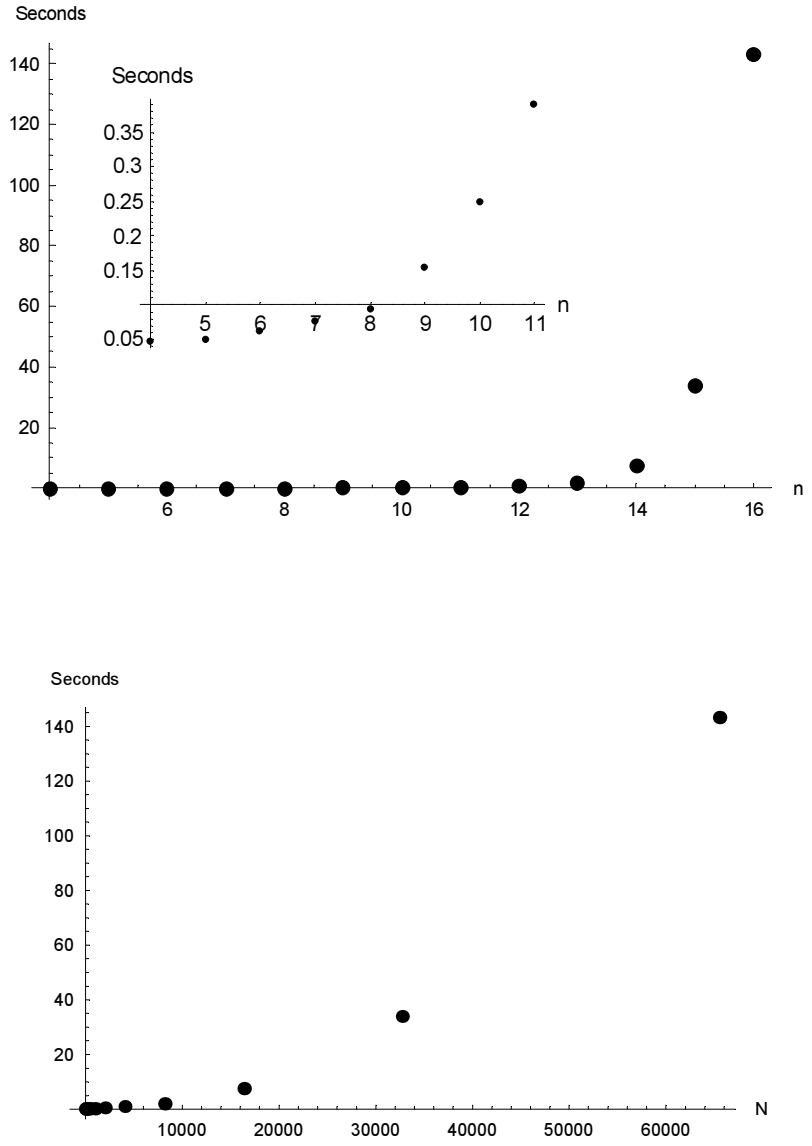


Figura 4.11: Tempos das simulações do algoritmo de Grover para uma base de dados clássica em função do número de qubits (n) e do tamanho da base de dados (N)

Computação Quântica, desde que se mantenham as implementações, tanto quanto possível, ao nível simbólico.

Versões futuras do simulador SQCS podem vir a constituir uma ferramenta útil para o desenvolvimento e verificação de algoritmos quânticos bem como no ensino e aprendizagem dos conceitos de Computação Quântica.

Epílogo

"*Everything that has a beginning*
comes to an end. "
Quintilian

Chegados a este ponto, não podemos deixar de sentir que as diversas e novas questões colocadas ao longo do trabalho de investigação aqui exposto ultrapassam em número e dificuldade as que tiveram resposta.

Os problemas encontrados na questão de relacionar o modelo de Circuitos Quânticos em Γ–qudits, proposto no capítulo 2 , com a Teoria da Complexidade no modelo de Computação Quântica baseado em qubits, bem como com o Modelo Clássico de Computação, são sem dúvida um incentivo à continuação de um trabalho de investigação nesta área.

De uma forma unificada, construímos no capítulo 3 duas classes de circuitos quânticos com profundidade constante e tamanho linear para a adição de dois números em sistemas redundantes. Estabelecemos ainda condições necessárias e suficientes para a aplicação de um algoritmo para a soma de um número polinomial números, sem propagação de dígitos de transporte e indicou-se a possibilidade de construir circuitos quânticos com profundidade constante para aproximar a soma de um número polinomial de números.

Em trabalho futuro, esperamos aproveitar o paralelismo exponencial e entrelaçamento para desenvolver algoritmos do tipo Deutsch-Jozsa em que os oráculos são circuitos quânticos para a adição de números, na tentativa de aproximar, de forma mais eficiente, as soluções de um conjunto de problemas difíceis, bem conhecidos, que envolvem o cálculo de somas.

Deixamos para este ponto algumas observações adicionais sobre o desenvolvimento de algoritmos quânticos para aritmética porque, até ao momento, não foi possível obter resultados conclusivos. De facto, um dos objectivos principais do trabalho de investigação que nos propusemos realizar consiste em estabelecer uma biblioteca de classes de algoritmos (circuitos) quânticos para a realização das várias operações aritméticas fundamentais, bem como funções trigonométricas, exponenciais e logarítmicas.

Em particular, trabalhou-se no sentido de averiguar a existência de circuitos quânticos para a divisão, em tempo constante, de números representados num sistema redundante. Embora se tenha concluído pela afirmativa, recorrendo a argumentos semelhantes aos apontados para o problema da adição, em tempo constante, de um número polinomial de números, consideramos esta solução não satisfatória. De facto, os algoritmos quânticos e correspondentes circuitos para a realização das diversas operações aritméticas obtêm-se essencialmente pela simulação quântica dos algoritmos existentes no contexto da Computação em Redes Neuronais, recorrendo à porta de *fanout* para simular a porta de *limiar*. Segundo este esquema, os recursos espaciais necessários a implementação da operação de divisão em tempo constante tendem a ser extremamente elevados.

Em alternativa, considerámos a possibilidade de adaptar ao contexto quântico os métodos clássicos de normalização aditiva, nomeadamente os métodos SRT (Sweeney, Robertson e Tocher). A adaptação directa deste método resulta num circuito quântico de profundidade linear. Contudo, resultados de simulações parecem indicar uma possível redução da profundidade dos circuitos para o nível logarítmico no tamanho dos operandos da divisão.

A existência de um Simulador de Computação Quântica permite o uso da experimentação no desenvolvimento de Algoritmos Quânticos. A construção do nosso simulador surgiu por pura necessidade durante o processo de desenvolvimento dos algoritmos aqui apresentados. O *Simulador Simbólico de Computação Quântica* pode ainda vir a revelar-se um instrumento útil no ensino da Computação Quântica.

Apêndices

Noções elementares $\langle \mathbf{A}|$

Seja $\mathbb{C}$ o corpo dos números complexos. Dado $\alpha \in \mathbb{C}$, α^* e $|\alpha|$ denotam, respectivamente, o *conjugado* complexo e o *módulo* de α. Seja $\mathcal{V}$ um espaço vectorial sobre $\mathbb{C}$.

Um *produto interno* em $\mathcal{V}$ é uma aplicação $(-,-) : \mathcal{V}^2 \to \mathbb{C}$, que satisfaz as seguintes condições[1]:

1. $\forall u \in \mathcal{V},\ (u,u) \geq 0$ e além disso $(u,u) = 0$ se e só se $u = 0$;
2. $\forall u, v \in \mathcal{V},\ (u,v) = (v,u)^*$;
3. $\forall u, v, w \in \mathcal{V},\ (u, v+w) = (u,v) + (u,w)$;
4. $\forall u, v \in \mathcal{V}, \forall \alpha \in \mathbb{C},\ (u, \alpha v) = \alpha (u,v)$.

O produto interno em $\mathcal{V}$ induz uma *norma*, $\|-\| : \mathcal{V} \to \mathbb{C}$, definida por

$$\|u\| = \sqrt{(u,u)},\ \forall u \in \mathcal{V}\,.$$

Para $u, v \in \mathcal{V}$ esta norma satisfaz a desigualdade triangular, $\|u, v\| \leq \|u\| + \|v\|$, bem como a desigualdade de Schwarz, $|(u,v)| \leq \|u\|\,\|v\|$.

Um espaço vectorial com produto interno, $\mathcal{V}$, diz-se *completo* relativamente à norma induzida pelo produto interno se toda a sequência de Cauchy é convergente, ou seja, sempre que $\{u_n\}$ é uma sequência em $\mathcal{V}$ tal que $\lim_{n,m\to+\infty} \|u_n - u_m\| = 0$ então existe $u \in \mathcal{V}$ tal que $\lim_{n\to+\infty} \|u_n\| = u$.

[1] Das propriedades 2 e 4 conclui-se que o produto interno é linear no segundo argumento e conjugado-linear no primeiro.

Definição A.1. Um *espaço de Hilbert*, $\mathcal{H}$, é um espaço vectorial sobre $\mathbb{C}$ equipado com um produto interno $(-,-) : \mathcal{H}\times\mathcal{H} \to \mathbb{C}$, completo relativamente à norma $\|u\| = \sqrt{(u,u)}$ induzida pelo produto interno.

Os elementos de um espaço de Hilbert $\mathcal{H}$ denominam-se *kets* e representam-se por $|\psi\rangle$, $|\phi\rangle$, etc.

Um funcional linear em $\mathcal{H}$ é uma aplicação linear de $\mathcal{H}$ no espaço complexo $\mathbb{C}$. O *espaço dual* de um espaço de Hilbert $\mathcal{H}$ denota-se por $\mathcal{H}^\dagger$ e corresponde ao espaço de Hilbert constituído pelos funcionais lineares em $\mathcal{H}$.

Os elementos do espaço dual denominam-se *bras* e denotam-se por $\langle\psi|$, $\langle\phi|$, etc.

Para um *bra* $\langle\phi|$ e um *ket* $|\psi\rangle$ o número complexo $\langle\phi|\,(|\psi\rangle)$, denota-se por $\langle\phi|\psi\rangle$.

Um importante resultado, conhecido pelo teorema de Riesz, garante que qualquer espaço de Hilbert de dimensão finita é isomorfo ao seu dual. O isomorfismo em causa $^\dagger : \mathcal{H} \to \mathcal{H}^\dagger$ é definido por $|\psi\rangle^\dagger = (|\psi\rangle\,, -)$.

Denotando o funcional linear $|\psi\rangle^\dagger$ por $\langle\psi|$ deduzem-se as seguintes propriedades:

1. $\langle\psi|\phi\rangle = (|\psi\rangle\,, |\phi\rangle)$;
2. $(\alpha\,|\psi\rangle)^\dagger = \alpha^*\,\langle\psi|$, para $\alpha \in \mathbb{C}$;
3. $\|\,|\psi\rangle\,\| = \sqrt{\langle\psi|\psi\rangle}$.

Um *operador linear*[2] $\mathbf{A}$ num espaço vectorial complexo $\mathcal{V}$ é uma aplicação $\mathbf{A} : \mathcal{V} \to \mathcal{V}$ tal que

$$\mathbf{A}(\alpha u + \beta v) = \alpha\mathbf{A}(u) + \beta\mathbf{A}(v),\ \forall u, v \in \mathcal{V}, \forall \alpha, \beta \in \mathbb{C}\,.$$

Formalmente, o produto tensorial de dois espaços vectoriais $\mathcal{V}_1$ e $\mathcal{V}_2$ é um espaço vectorial $\mathcal{V}$ juntamente com uma aplicação bilinear $\otimes : \mathcal{V}_1 \times \mathcal{V}_2 \to \mathcal{V}$ que verifica a seguinte propriedade universal: para quaisquer espaço vectorial $\mathcal{V}'$ e aplicação bilinear $\otimes' : \mathcal{V}_1 \times \mathcal{V}_2 \to \mathcal{V}'$, existe uma única aplicação linear $\mathbf{A}$ de $\mathcal{V}$ em $\mathcal{V}'$ tal que $\otimes'(u,v) = \mathbf{A}(\otimes(u,v))$, para $u \in \mathcal{V}_1, v \in \mathcal{V}_2$.

[2] Também designado transformação linear.

Como alternativa a esta definição abstracta mas independente das bases em cada um dos espaços, considera-se, num compromisso entre rigor e clareza, a seguinte definição:

Definição A.2. O *produto tensorial* $\mathcal{H}\otimes\mathcal{K}$ dos espaços de Hilbert $\mathcal{H}$ e $\mathcal{K}$ é o "menor" espaço de Hilbert que satisfaz:

1. $(h_1+h_2)\otimes k = h_1\otimes k + h_2\otimes k,\ \ \forall h_1,h_2\in\mathcal{H},\,\forall k\in\mathcal{K}$;
2. $h\otimes(k_1+k_2) = h\otimes k_1 + h\otimes k_2,\ \ \forall h\in\mathcal{K},\,\forall k_1,k_2\in\mathcal{K}$;
3. $\alpha(h\otimes k) = (\alpha h)\otimes k = h\otimes(\alpha k),\,\forall h\in\mathcal{H},\,\forall k\in\mathcal{K},\,\forall\alpha\in\mathbb{C}$.

Se $\{h_1,h_2,\ldots,h_m\}$ e $\{k_1,k_2,\ldots,k_n\}$ são, respectivamente, bases dos espaços de Hilbert $\mathcal{H}$ e $\mathcal{K}$ então $\{h_i\otimes k_j | 1\leq i\leq m, 1\leq j\leq n\}$ é uma base de $\mathcal{H}\otimes\mathcal{K}$. Note-se então que $\dim(\mathcal{H}\otimes\mathcal{K}) = \dim(\mathcal{H})\cdot\dim(\mathcal{K})$.

O *adjunto* $\mathbf{A}^\dagger$ de um operador $\mathbf{A}$ é um operador tal que

$$(\mathbf{A}^\dagger|\phi\rangle\,,|\psi\rangle) = (|\phi\rangle\,,\mathbf{A}|\psi\rangle),\ \forall|\phi\rangle\,,|\psi\rangle\ .$$

É possível associar a cada operador linear $\mathbf{A}$ em $\mathcal{H}$ um operador linear em $\mathcal{H}^\dagger$, denotado também por $\mathbf{A}$, definido por

$$\langle\phi|\longmapsto\langle\phi|\,\mathbf{A},$$

em que $\langle\phi|\,\mathbf{A}$ é o funcional linear definido por $(\langle\phi|\,\mathbf{A})(|\psi\rangle) = \langle\phi|\,(\mathbf{A}|\psi\rangle),\,\forall|\psi\rangle$. Esta última expressão, conhecida por lei associativa de Dirac, permite concluir que a expressão $\langle\phi|\,\mathbf{A}\,|\psi\rangle$ não é ambígua. Note-se ainda que $(\mathbf{A}|\psi\rangle)^\dagger = \langle\psi|\,\mathbf{A}^\dagger$.

Um operador $\mathbf{U}$ num espaço de Hilbert $\mathcal{H}$ diz-se *unitário* se $\mathbf{U}^\dagger = \mathbf{U}^{-1}$. O conjunto dos operadores unitários num espaço de Hilbert $\mathcal{H}$ denota-se por $\mathcal{U}(\mathcal{H})$.

O produto tensorial de dois operadores $\mathbf{A}$ e $\mathbf{B}$ definidos respectivamente sobre os espaços de Hilbert $\mathcal{H}$ e $\mathcal{K}$ é um operador em $\mathcal{H}\otimes\mathcal{K}$, denotado por $\mathbf{A}\otimes\mathbf{B}$ e definido por

$$(\mathbf{A}\otimes\mathbf{B})\,(|a_j\rangle\otimes|b_k\rangle) = \mathbf{A}\,|a_j\rangle\otimes\mathbf{B}\,|b_k\rangle$$

onde $\{|a_j\rangle\otimes|b_k\rangle\}$ denota um base de $\mathcal{H}\otimes\mathcal{K}$. Por indução generaliza-se esta definição para o produto tensorial de um qualquer número de operadores unitários. Note-se que o produto tensorial de dois operadores unitários é ainda um operador unitário.

A.1 Observáveis

Em Mecânica Quântica, um *observável* é um operador Hermitiano (também designado por auto-adjunto) num espaço de Hilbert $\mathcal{H}$, i.e, um operador linear $\mathbf{A}$ tal que $\mathbf{A}^\dagger = \mathbf{A}$.

Um *operador de projecção* é um operador linear $\mathbf{P}$ definido num espaço de Hilbert $\mathcal{H}$ tal que $\mathbf{P}^2 = \mathbf{P}$. Designa-se por *projector* um operador de projecção Hermitiano, ou seja um operador linear $\mathbf{P}$ tal que $\mathbf{P}^2 = \mathbf{P}$ e $\mathbf{P} = \mathbf{P}^\dagger$. Seja $\mathcal{P}$ o subespaço de $\mathcal{H}$ dado pela imagem de $\mathbf{P}$. Diz-se que $\mathbf{P}$ é o projector do subespaço $\mathcal{P}$ e que $\mathbf{P}$ projecta $\mathcal{H}$ em $\mathcal{P}$.

Seja $\mathbf{P}$ um projector do subespaço $\mathcal{P}$ de um espaço de Hilbert $\mathcal{H}$ e considere-se uma base ortonormada de $\mathcal{P}$: $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{k-1}\rangle$. Nestas condições, é possível escrever o projector $\mathbf{P}$ na forma

$$\mathbf{P} = \sum_{j=0}^{k-1} |\psi_j\rangle\langle\psi_j| \quad .$$

Note-se que $\mathbf{P}_j = |\psi_j\rangle\langle\psi_j|$ é, para cada j, o projector para o subespaço de $\mathcal{H}$ gerado por $|\psi_j\rangle$.

Um *valor próprio* de um operador linear $\mathbf{A}$ é um número complexo λ para o qual existe $|\psi\rangle \in \mathcal{H}$ tal que $\mathbf{A}|\psi\rangle = \lambda|\psi\rangle$. Diz-se então que $|\psi\rangle$ é um *ket próprio* de $\mathbf{A}$ associado ao valor próprio λ.

O *espaço próprio* correspondente ao valor próprio λ é o subespaço $\mathcal{P}_\lambda$ de $\mathcal{H}$ constituído por todos os kets próprios associados a λ, i.e.,

$$\mathcal{P}_\lambda = \{|\psi\rangle \,:\, \mathbf{A}|\psi\rangle = \lambda|\psi\rangle\} \ .$$

O projector para o subespaço $\mathcal{P}_\lambda$ denota-se por $\mathbf{P}_\lambda$.

Teorema A.1. Os valores próprios λ_j de um observável $\mathbf{A}$ são números reais. Além disso kets próprios associados a valores próprios distintos são ortogonais.

Tanto os observáveis como os operadores unitários fazem parte da classe dos *operadores normais*. Diz-se que um operador linear, $\mathbf{A}$, é normal se comuta com o seu operador adjunto (i.e., $\mathbf{A}\mathbf{A}^\dagger = \mathbf{A}^\dagger\mathbf{A}$). Entre as muitas propriedades dos operadores normais destaca-se a seguinte.

Teorema A.2 (Decomposição Espectral)**.** Sejam $\lambda_0, \lambda_1, \ldots, \lambda_{k-1}$ os k valores próprios distintos de um operador linear $\mathbf{A}$ de um espaço de Hilbert $\mathcal{H}$. O operador $\mathbf{A}$ é normal se e só se admite a decomposição espectral

$$\mathbf{A} = \sum_{j=0}^{k-1} \lambda_j \mathbf{P}_{\lambda_j}.$$

Uma outra condição necessária e suficiente para que um operador linear $\mathbf{A}$ seja normal é que o espaço de Hilbert $\mathcal{H}$ seja a soma directa dos subespaços próprios de $\mathbf{A}$, i.e.,

$$\mathcal{H} = \mathcal{P}_{\lambda_0} \oplus \mathcal{P}_{\lambda_1} \oplus \ldots \oplus \mathcal{P}_{\lambda_{k-1}}.$$

Decorre do teorema anterior que os projectores $\mathbf{P}_{\lambda_0}, \mathbf{P}_{\lambda_1}, \ldots, \mathbf{P}_{\lambda_{k-1}}$ associados a um operador normal são mutuamente ortogonais, i.e, $\mathbf{P}_{\lambda_i}\mathbf{P}_{\lambda_j} = \mathbf{0}$ para $i \neq j$, e constituem um conjunto completo, i.e, $\sum_{j=0}^{k-1} \mathbf{P}_{\lambda_j} = \mathbf{I}$, onde $\mathbf{I}$ denota o operador identidade no espaço de Hilbert $\mathcal{H}$. Daqui resulta que qualquer vector $|\psi\rangle \in \mathcal{H}$ admite a decomposição

$$|\psi\rangle = \sum_{j=0}^{k-1} \left(\mathbf{P}_{\lambda_j} |\psi\rangle\right).$$

Assim, se $\mathbf{A}$ é um qualquer operador linear normal, então existe uma base ortonormada do espaço de Hilbert subjacente constituída pelos kets próprios de $\mathbf{A}$.

O operador $\mathbf{A}$ é ainda diagonalizável. De facto, para cada $j \in [1 \,..\, k]$, seja

$$e_{j0}, e_{j1}, \cdots, e_{j(m_j-1)}$$

uma base ortonormada do espaço próprio $\mathcal{P}_{\lambda_j}$. Então

$$e_{00}, e_{01}, \cdots, e_{0(m_0-1)},\ e_{10}, e_{11}, \cdots, e_{1(m_1-1)},\ \ldots,\ e_{(k-1)0}, e_{(k-1)1}, \cdots, e_{(k-1)(m_{k-1}-1)}$$

constitui uma base ortonormada de $\mathcal{H}$ e, em termos desta base, a representação do operador $\mathbf{A}$ é dado por uma matriz diagonal $k \times k$, com diagonal

$$\underbrace{\lambda_0 \ldots \lambda_0}_{m_0}\ \underbrace{\lambda_1 \ldots \lambda_1}_{m_1}\ \cdots\ \underbrace{\lambda_{k-1} \ldots \lambda_{k-1}}_{m_{k-1}}.$$

Seja $\mathbf{A}$ um operador linear normal num espaço de Hilbert $\mathcal{H}$. Diz-se que um valor próprio λ é *degenerado* se o espaço próprio correspondente $\mathcal{P}_\lambda$ tem dimensão superior a 1. Caso contrário o valor próprio diz-se não degenerado.

Diz-se ainda que $\mathbf{A}$ é um operador não degenerado se todos os seus valores próprios são não degenerados. Caso contrário diz-se um *operador degenerado*.

Se λ_j é um valor próprio degenerado então $|\lambda_j, 0\rangle, |\lambda_j, 1\rangle, \ldots, |\lambda_j, m_j - 1\rangle$ denota uma base ortonormada do espaço próprio associado $\mathcal{P}_{\lambda_j}$. No caso de λ_j ser um valor próprio não degenerado tal base denota-se simplesmente por $|\lambda_j\rangle$.

Com a notação anterior a decomposição espectral de $\mathbf{A}$ assume a seguinte forma

$$\mathbf{A} = \sum_{j=0}^{k-1} \lambda_j \sum_{i=0}^{m_j-1} |\lambda_j, i\rangle \langle \lambda_j, i|.$$

No caso do operador $\mathbf{A}$ ser não degenerado, a decomposição espectral é simplesmente

$$\sum_{j=0}^{k-1} \lambda_j |\lambda_j\rangle \langle \lambda_j| .$$

Decomposição de operadores em $\langle \mathbf{B}|$ produtos tensoriais

A representação de operadores lineares no simulador SQCS baseia-se na definição de regras algébricas. Cada regra especifica a acção de um operador sobre um estado base. A simulação da acção de um operador sobre um estado geral (combinação linear de estados base) realiza-se, em última instância, por aplicação directa da linearidade (associatividade, distributividade, etc).

No entanto, a simulação eficiente da acção de um operador linear é uma tarefa não trivial que depende de existir (e se conhecer!) uma decomposição do operador na forma de um produto tensorial de operadores com acção local (definidos sobre um pequeno número de qudits). Com os exemplos seguintes pretende-se, precisamente, elucidar estas considerações.

B.1 Decomposição do operador de Walsh-Hadamard

A implementação directa no *Mathematica* da definição do operador de Walsh-Hadamard (4.1) é claramente ineficiente. A título de exemplo, considere-se o problema de simular a acção da composição de um operador linear, $\mathbf{U}$, com $\mathbf{H}^{\otimes n}$ sobre um sistema quântico inicialmente no estado base $|i\rangle$:

$$\mathbf{U} \cdot \mathbf{H}^{\otimes n} |i\rangle = \mathbf{U} \left(\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} |j\rangle \right) = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} \mathbf{U} |j\rangle \ . \tag{B.1}$$

Qualquer implementação da expressão mais à direita nesta última fórmula, na qual o operador $\mathbf{U}$ aparece um número exponencial de vezes, terá inevitavelmente complexidade temporal

$\mathcal{O}(2^n)$. (*ipsis verbis* relativamente à complexidade espacial.)

O problema da complexidade em (B.1) é sanado ao se observar que o operador de Walsh-Hadamard, como a notação sugere, é o produto tensorial de operadores de Hadamard.

De facto, considere-se inicialmente a decomposição de um estado base $|i\rangle$ na forma de um produto tensorial:

$$|i\rangle = |i_{n-1}\rangle \otimes \cdots \otimes |i_1\rangle \otimes |i_0\rangle \ , \tag{B.2}$$

onde cada *ket* $|i_k\rangle$ é um estado base do espaço de Hilbert $\mathcal{H}_2$. Este produto corresponde à representação binária de i em n bits, calculável em tempo linear em n (no *Mathematica* com a função `IntegerDigits[i,2,n]`). Aplique-se em seguida o operador de Hadamard a cada um dos n kets no produto (B.2):

$$\begin{aligned}
\mathbf{H}^{\otimes n}|i\rangle &= \mathbf{H}^{\otimes n}\left(|i_{n-1}\rangle \otimes |i_{n-2}\rangle \otimes \cdots \otimes |i_0\rangle\right) \\
&= \mathbf{H}|i_{n-1}\rangle \otimes \mathbf{H}|i_{n-2}\rangle \otimes \cdots \otimes \mathbf{H}|i_0\rangle \\
&= \frac{|0\rangle + (-1)^{i_{n-1}}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + (-1)^{i_0}|1\rangle}{\sqrt{2}} \\
&= \frac{\left(|0\rangle + (-1)^{i_{n-1}}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + (-1)^{i_0}|1\rangle\right)}{2^{n/2}} \ .
\end{aligned} \tag{B.3}$$

A complexidade da última expressão em (B.3) cresce apenas linearmente com n.

Mais geralmente, considere-se um qualquer estado produto $|\psi\rangle = \bigotimes_{i=0}^{n-1}|\psi_i\rangle$, em que $|\psi_i\rangle \in \mathcal{H}_2$. É possível calcular o estado $\mathbf{H}^{\otimes n}|\psi\rangle$ em tempo linear em n, uma vez que

$$\mathbf{H}^{\otimes n}|\psi\rangle = \bigotimes_{i=0}^{n-1} \mathbf{H}|\psi_i\rangle \ . \tag{B.4}$$

Relativamente à simulação eficiente do problema considerado inicialmente, acção da composição de um operador unitário $\mathbf{U}$ com $\mathbf{H}^{\otimes n}$, note-se que:

$$\mathbf{U} \cdot \mathbf{H}^{\otimes n}|i\rangle = \mathbf{U}\left(\mathbf{H}|i_{n-1}\rangle \otimes \mathbf{H}|i_{n-2}\rangle \otimes \cdots \otimes \mathbf{H}|i_0\rangle\right). \tag{B.5}$$

Assim o problema reduz-se agora à existência e conhecimento de uma decomposição para o operador $\mathbf{U}$ na forma de um produto tensorial. De facto, admita-se a existência de uma decomposição para $\mathbf{U}$ num produto tensorial de m factores ($1 \ll m \leq n$): $\mathbf{U} = \bigotimes_{j=0}^{m-1}\mathbf{U}_j$

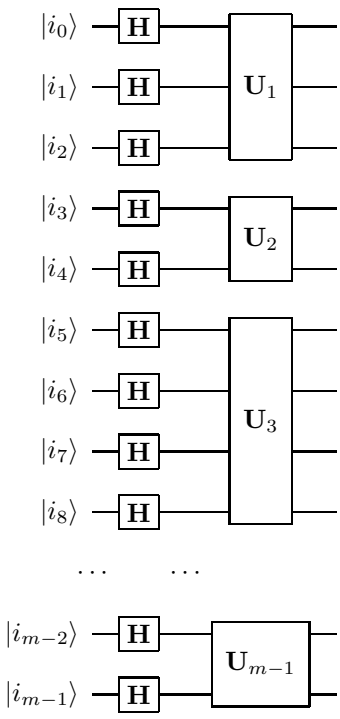


Figura B.1: Esquema da acção de $\mathbf{H}^{\otimes n}$ seguida da acção de um operador $\mathbf{U}$ que admita uma decomposição em m factores.

onde $\mathbf{U}_j$ é um operador unitário em $\mathcal{H}_{2^{d_j}}$ ($\sum_{j=0}^{m-1} d_j = n$). Por simples manipulação algébrica de (B.5) conclui-se que

$$\mathbf{U} \cdot \mathbf{H}^{\otimes n} |i\rangle = \bigotimes_{j=1}^{m} \mathbf{U}_j \bigotimes_{k=0}^{d_j-1} \mathbf{H} |i_{s_k+k}\rangle \,, \tag{B.6}$$

onde $s_0 = 0$ e $s_k = \sum_{l=0}^{k-1} d_l$ para $k \geq 1$.

Cada um dos m blocos presentes em (B.6) consiste na acção local do operador $\mathbf{U}_j$ sobre d_j qubits como se ilustra na figura B.1. É assim possível, nestas condições, simular a composição de $\mathbf{U}$ com $\mathbf{H}^{\otimes n}$ em tempo (e espaço) $\mathcal{O}(n)$.

B.2 Decomposição do operador Produto Externo

Sejam $|i\rangle$ e $|j\rangle$ estados base. Considere-se um qualquer estado produto $|\psi\rangle = \bigotimes_{s=0}^{n-1} |\psi_s\rangle$, onde $|\psi_s\rangle \in \mathcal{H}_2$. É possível simular a acção do operador produto externo $|i\rangle\langle j|$ sobre $|\psi\rangle$ em tempo $\mathcal{O}(n)$ da forma seguinte.

Inicialmente determinam-se as representações binárias para i e j, $|i\rangle = \bigotimes_{s=0}^{n-1} |i_s\rangle$ e $\langle j| = \bigotimes_{s=0}^{n-1} \langle j_s|$. Em seguida, utiliza-se a propriedade

$$\begin{aligned} |i\rangle\langle j|\,|\psi\rangle &= \left(\bigotimes_{s=0}^{n-1} |i_s\rangle\right)\left(\bigotimes_{s=0}^{n-1} \langle j_s|\right)|\psi\rangle = \left(\bigotimes_{s=0}^{n-1} |i_s\rangle\langle j_s|\right)|\psi\rangle \\ &= \left(\bigotimes_{s=0}^{n-1} |i_s\rangle\langle j_s|\right)\left(\bigotimes_{s=0}^{n-1} |\psi_s\rangle\right) = \bigotimes_{s=0}^{n-1} |i_s\rangle\langle j_s|\,|\psi_s\rangle \ . \end{aligned}$$

Note-se que a alternativa que consiste em expandir inicialmente o estado $|\psi\rangle = \bigotimes_{s=0}^{n-1} |\psi_s\rangle$ na forma de um estado $\sum_{k=0}^{2^n-1} \alpha_k |k\rangle$ e em seguida utilizar directamente a definição do produto externo(4.2) tem complexidade temporal (e espacial) $\mathcal{O}(2^n)$.

Bibliografia

[1] Dave Bacon, Andrew M. Childs e Wim van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. 2005. arXiv:quant-ph/0504083.

[2] Stephen D. Bartlett, Hubert de Guise e Barry C. Sanders. Quantum encodings in spin systems and harmonic oscillators. *Physical Review A*, 65:1–4, 2002.

[3] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22(5):563–591, May 1980. doi: 10.1007/BF01011339.

[4] Paul Benioff. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 29(3):515–546, November 1982.

[5] Paul Benioff. Quantum mechanical models of turing machines that dissipate no energy. *Phys. Rev. Lett.*, 48(23):1581–1585, June 1982.

[6] Ethan Bernstein e Umesh Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26 (5):1411–1473, 1997. ISSN 0097-5397. doi: 10.1137/S0097539796300921.

[7] Eli Biham, Ofer Biham, David Biron, Markus Grassl e Daniel A. Lidar. Grover's quantum search algorithm for an arbitrary initial amplitude distribution. *Phys. Rev. A*, 60:2742, 1999. doi: 10.1103/PhysRevA.60.2742.

[8] G. Brassard, P. Høyer, M. Mosca e A. Tapp. Quantum amplitude amplification and

estimation. In S. J. Lomonaco e H. E. Brandt, editors, *Quantum Computation and Information*, volume 305 of *Contemporary Mathematics Series*. AMS, 2002.

[9] Jean-Luc Brylinski e Ranee Brylinski. Universal quantum gates. 2001. arXiv:quant-ph/0108062.

[10] Stephen S. Bullock, Dianne P. O'Leary e Gavin K. Brennen. Asymptotically optimal quantum circuits for d-level systems. *Physical Review Letters*, 94:230502, 2005. doi: 10.1103/PhysRevLett.94.230502.

[11] Sorin Cotofana e Stamatis Vassiliadis. Signed digit counters with neural networks. In *Proc. Neurap'97*, pages 55–62, March 1997.

[12] Sorin Cotofana e Stamatis Vassiliadis. Signed digit addition and related operations with threshold logic. *IEEE Transactions on Computers*, 49(3):193–207, 2000. ISSN 0018-9340. doi: 10.1109/12.841124.

[13] Jamil Daboul, Xiaoguang Wang e Barry C. Sanders. Quantum gates on hybrid qudits. *Journal of Physics A: Mathematical and General*, 36(10):2525–2536, 2003.

[14] Andreas de Vries. jquantum. 2004. http://jquantum.sourceforge.net/.

[15] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Ser. A*, A400:97–117, 1985.

[16] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London Ser. A*, 425(1868):73 – 90, 1989.

[17] David Deutsch e Richard Jozsa. Rapid solution of problems by quantum computation. *Royal Society of London Proceedings Series A*, 439:553–558, December 1992.

[18] Thomas G. Draper. Addition on a quantum computer. 2000.

[19] Thomas G. Draper, Samuel A. Kutin, Eric M. Rains e Krysta M. Svore. A logarithmic-depth quantum carry-lookahead adder. 2004.

[20] Paul Dumais e Hugo Touchette. Qucalc. 2004. http://crypto.cs.mcgill.ca/QuCalc/.

[21] Mark Ettinger e Peter Høyer. The quantum query complexity of the hidden subgroup problem is polynomial. 2004. `arXiv:quant-ph/0401083`.

[22] M. Fang, S. Fenner, F. Green, S. Homer e Y. Zhang. Quantum lower bounds for fanout. 2003. `arXiv:quant-ph/0312208`.

[23] Stephen Fenner, Frederic Green, Steven Homer e Yong Zhang. Bounds on the power of constant-depth quantum circuits. 2003. `arXiv:quant-ph/0312209`.

[24] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–468, 1982.

[25] P. Gossett. Quantum carry-save arithmetic. August 1998. `arXiv:quant-ph/9808061`.

[26] Frederic Green, Steven Homer, Cristopher Moore e Christopher Pollett. Counting, fanout, and the complexity of quantum acc. *Quantum Information and Computation*, 2(1):35–65, 2002.

[27] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th Annual ACM Symposium on the Theory of Computing*, pages 212–219, May 1996.

[28] Peter Høyer. On arbitrary phases in quantum amplitude amplification. 2000. `arXiv:quant-ph/0006031`.

[29] Peter Høyer e Robert Špalek. Quantum fan-out is powerful. *Theory of Computing*, 1(5): 81–103, 2005.

[30] Markus Hunziker e David A. Meyer. Quantum algorithms for highly structured search problems. *Quantum Information Processing*, 1(3):145–154, 2002.

[31] Richard Jozsa. Quantum factoring, discrete logarithms and the hidden subgroup problem. January 2000.

[32] Faisal Shah Khan e Marek Perkowski. Synthesis of multi-qudit hybrid and d-valued quantum logic circuits by decomposition. 2005.

[33] A. Yu. Kitaev, A.H. Shen e M.N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[34] Alexei Kitaev e John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 608–617, New York, NY, USA, 2000. ACM Press. ISBN 1-58113-184-4. doi: 10.1145/335305.335387.

[35] Cristopher Moore e Martin Nilsson. Some notes on parallel quantum computation. 1998. arXiv:quant-ph/9804034.

[36] Michele Mosca e Christof Zalka. Exact quantum Fourier transforms and discrete logarithm algorithms. 2003.

[37] Ashok Muthukrishnan e C. R. Stroud. Multivalued logic gates for quantum computation. *Phys. Rev. A*, 62(5):052309, Oct 2000. doi: 10.1103/PhysRevA.62.052309.

[38] Yumi Nakajima, Yasuhito Kawano e Hiroshi Sekigawa. A new algorithm for producing quantum circuits using kak decompositions. *Quantum Information & Computation (Rinton Press)*, 6(1):67–80, 2005.

[39] Michael A. Nielsen e Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambrige University Press, 2000.

[40] Harumichi Nishimura. Computational complexity of uniform quantum circuit families and quantum turing machines. *International Journal of Foundations of Computer Science*, 14(1-2):853–870, 2003. ISSN 0304-3975. doi: 10.1142/S0129054103002059.

[41] Harumichi Nishimura e Masanao Ozawa. Computational complexity of uniform quantum circuit families and quantum turing machines. *Theor. Comput. Sci.*, 276(1-2):147–181, 2002. ISSN 0304-3975. doi: 10.1016/S0304-3975(01)00111-6.

[42] Harumichi Nishimura e Masanao Ozawa. Perfect computational equivalence between quantum turing machines and finitely generated uniform quantum circuit families. 2005. arXiv:quant-ph/0511117.

[43] Harumichi Nishimura e Masanao Wim van Dam Ozawa. Uniformity of quantum circuit families for error-free algorithms. *Theoretical Computer Science*, 332(1-3):487–496, February 2005. doi: 10.1016/j.tcs.2004.12.020.

[44] Behrooz Parhami. Generalized signed-digit number systems: A unifying framework for redundant number representations. *IEEE Transactions on Computers*, 39:89–98, January 1990. doi: 10.1109/12.46283.

[45] António Pereira. Um modelo unificado de aritmética digital. Master's thesis, Universidade de Coimbra, 1998.

[46] António Pereira e Rosália Rodrigues. O algoritmo quântico de Shor para o problema da factorização. Cadernos de matemática, Departamento de Matemática da Universidade de Aveiro, 2004.

[47] Helge Rosé et al. Fraunhofer quantum computing simulator. 2005. http://www.qc.fraunhofer.de/.

[48] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134, 1994. doi: 10.1109/SFCS.1994.365700.

[49] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. doi: 10.1137/S0097539795293172.

[50] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997. ISSN 0097-5397. doi: http://dx.doi.org/10.1137/S0097539796298637.

[51] David R. Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, Los Alamitos, CA, 1994. Institute of Electrical and Electronic Engineers Computer Society Press.

[52] V. Vedral, A. Barenco e A. Ekert. Quantum networks for elementary arithmetic operations. 1995. arXiv:quant-ph/9511018.

[53] J. von Neumann. *Mathematical Foundation of Quantum Mechanics*. Princeton University Press, 1955.

[54] Stephen Wolfram. *TheMathematica Book, Fifth Edition*. Wolfram Media, Inc., 2003.

[55] A. Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361, 1993. doi: 10.1109/SFCS.1993.366852.

Índice Remissivo